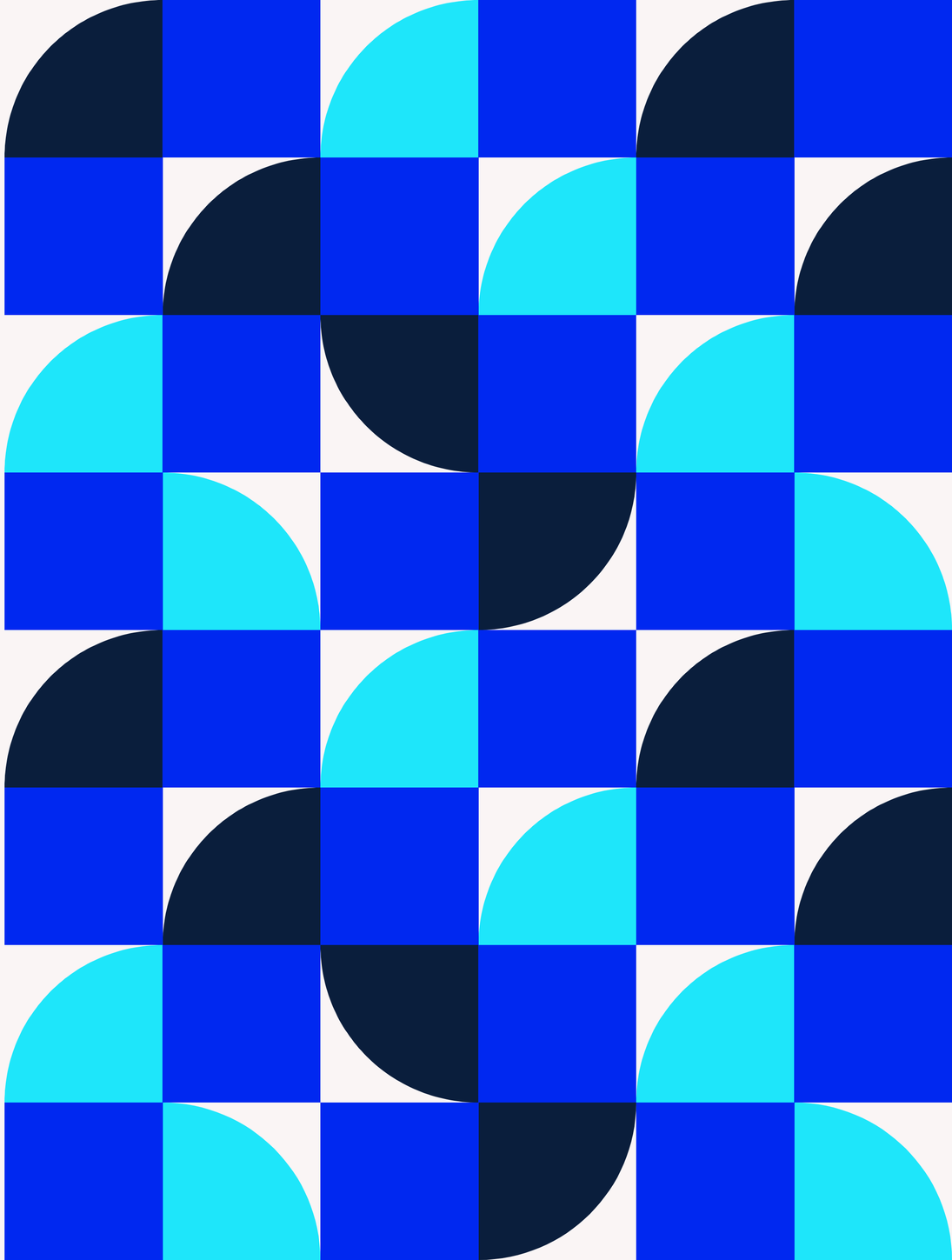
F-Secure

Two More Ways the Quarantine Attribute Can Fail Us

Rasmus Sten & Arthur Valiev
F-Secure macOS Endpoint Protection R&D
October 12, 2023





Agenda

1. Introduction
2. The story of an accidental vulnerability discovery (CVE-2023-27943)
3. Archive extraction and long file paths (CVE-2021-1810)
4. Final thoughts

Introduction: Glossary

macOS Gatekeeper

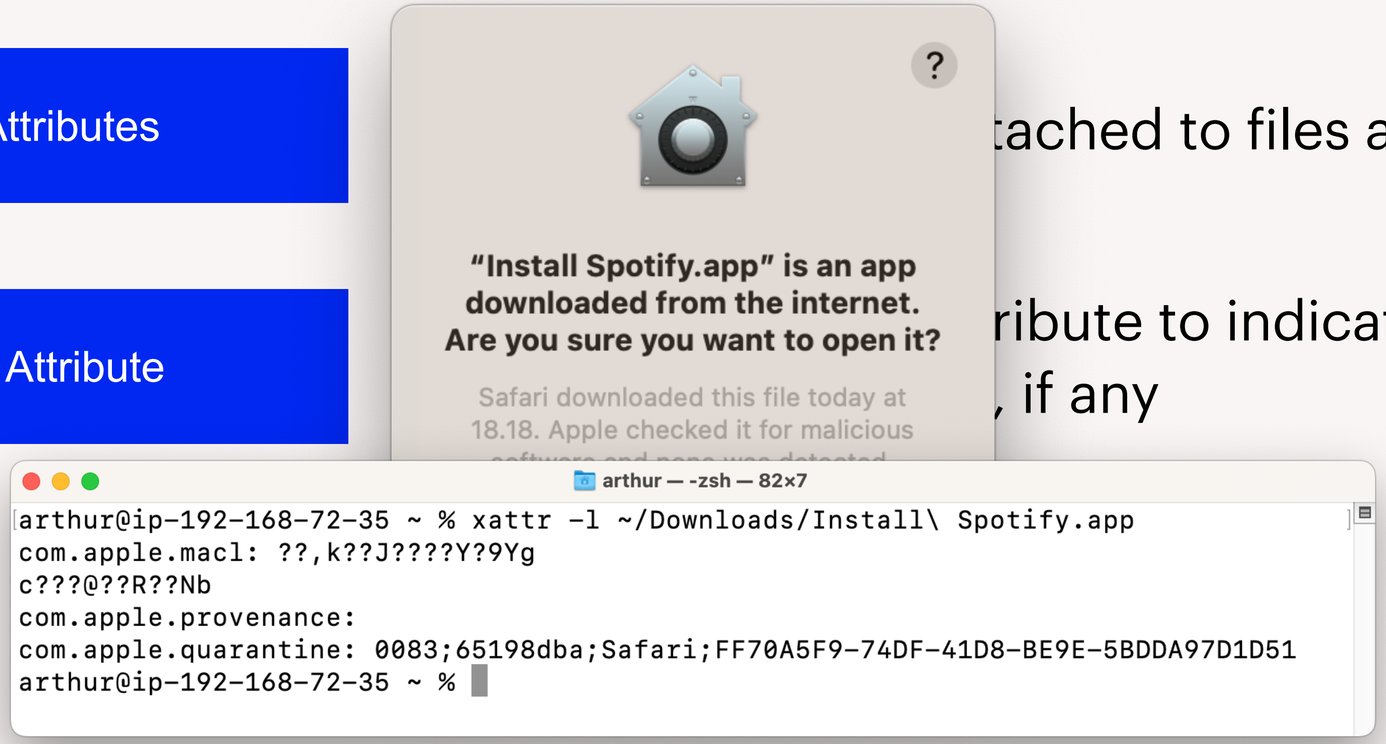
Prevents unauthorized software from running

Extended Attributes

tached to files and folders

Quarantine Attribute

ribute to indicate the
, if any



Introduction: Glossary

Launch Services

Launch Services is a macOS system component used to manage launching/opening of applications, documents, etc. It acts as a central hub that facilitates the interaction between the user, the operating system, and the applications installed on the system.

Launch Services maintains a registry of all installed applications on the system and can help the system determine the appropriate application to handle a specific file or URL based on its file type or scheme.

LSFileQuarantineEnabled Info.plist flag

Files created or downloaded by an application that has the LSFileQuarantineEnabled flag set to true in the Info.plist will have the com.apple.quarantine attribute. By default, the LSFileQuarantineEnabled is set to false.

When quarantining files, the system automatically associates the timestamp, app name, and the bundle identifier with the quarantined file whenever possible.

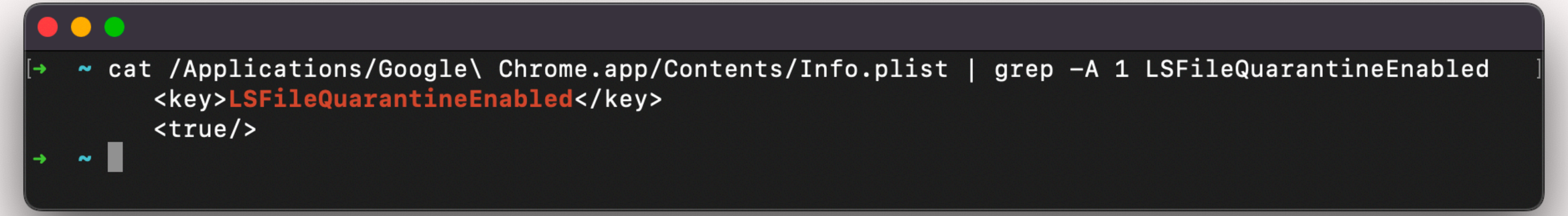
Presence of quarantine attribute is the primary signal for macOS to active protection mechanisms like Gatekeeper.

Vulnerability discovery

Google Chrome downloads a file from the Internet

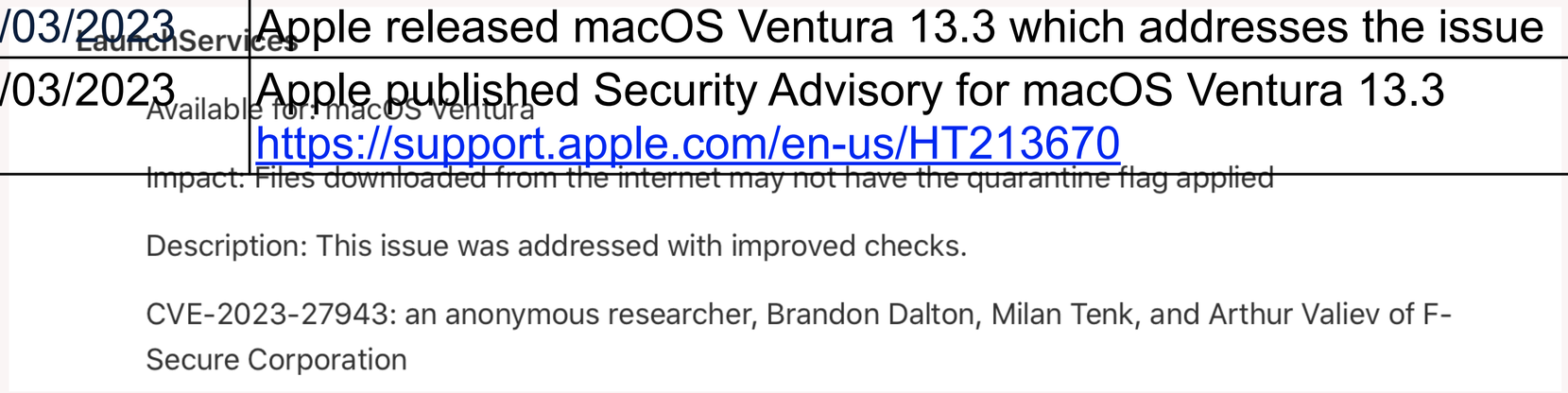
macOS automatically sets Quarantine attribute to all files Google Chrome touches on disk

macOS Gatekeeper checks validity of the file



Disclosure timeline

17/01/2023	Vulnerability discovered during F-Secure Endpoint Security product beta release testing on macOS Ventura
17/01/2023	Vulnerability reported to Apple Product Security
14/02/2023	F-Secure releases Mac Endpoint Security product update 19.0 with improved detection capabilities to mitigate macOS vulnerability
24/03/2023	Apple released macOS Ventura 13.3 which addresses the issue
24/03/2023	Apple published Security Advisory for macOS Ventura 13.3 https://support.apple.com/en-us/HT213670


LaunchServices

Available for: macOS Ventura

Impact: Files downloaded from the internet may not have the quarantine flag applied

Description: This issue was addressed with improved checks.

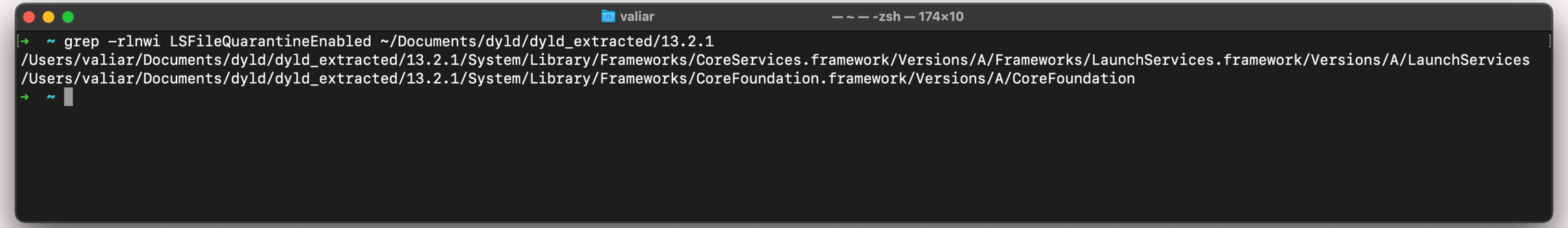
CVE-2023-27943: an anonymous researcher, Brandon Dalton, Milan Tenk, and Arthur Valiev of F-Secure Corporation

F-Secure

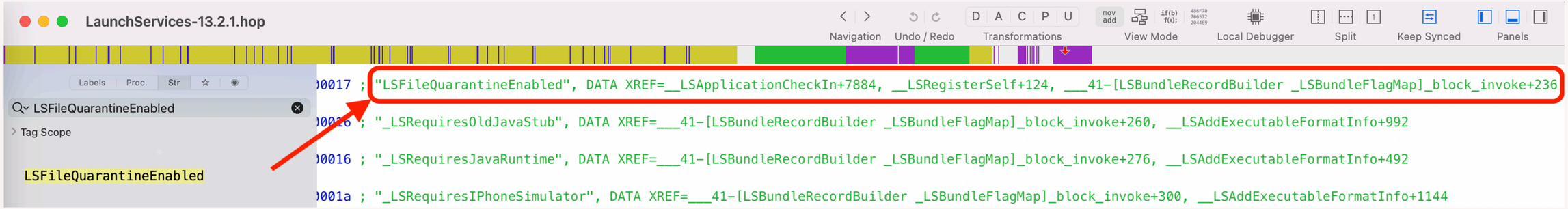
Demo

Investigation: system libraries binaries extraction from dyld cache

- Use dyld-shared-cache-extractor to extract binaries of system libraries from dyld cache
- Search for mentions of LSFileQuarantineEnabled
- Hopper time



Investigation: Hopper Disassembler

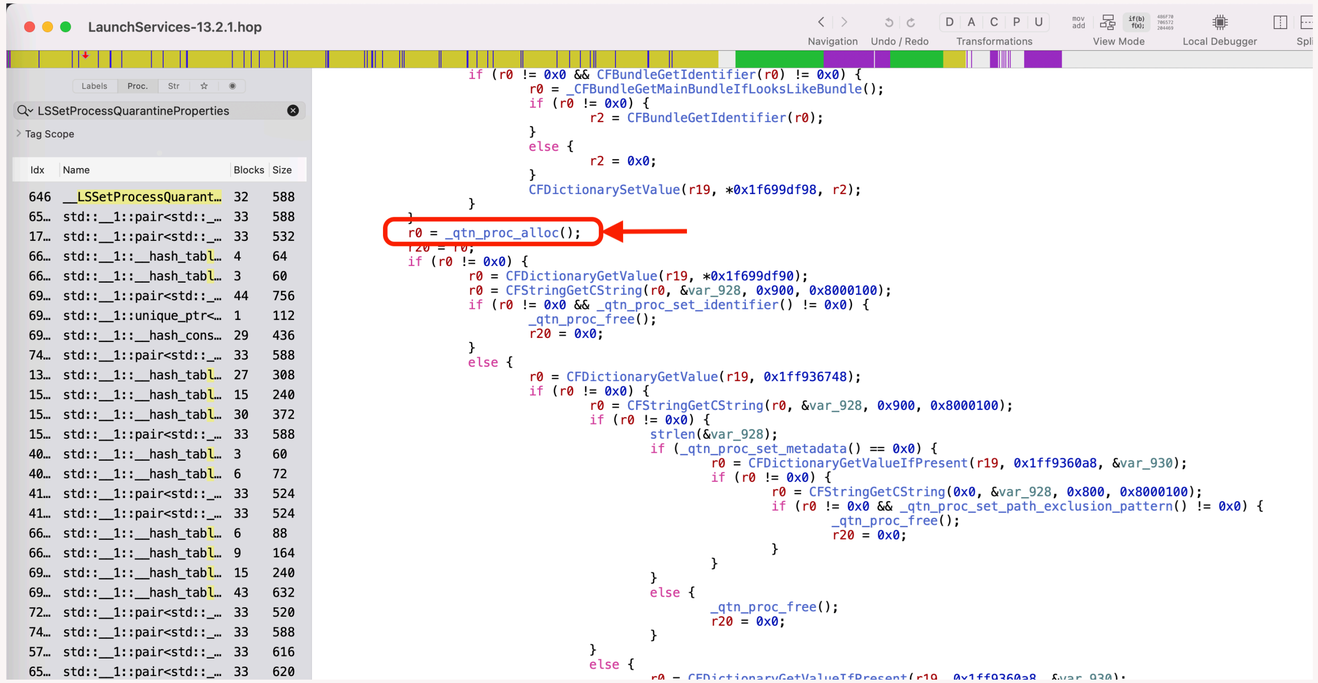


- __LSApplicationCheckIn handles application checkin to lsd (XPC)
- __LSRegisterSelf calls into __LSSetProcessQuarantineProperties which then collects app metadata and passes it along to libquarantine dylib to complete app self-registration routine

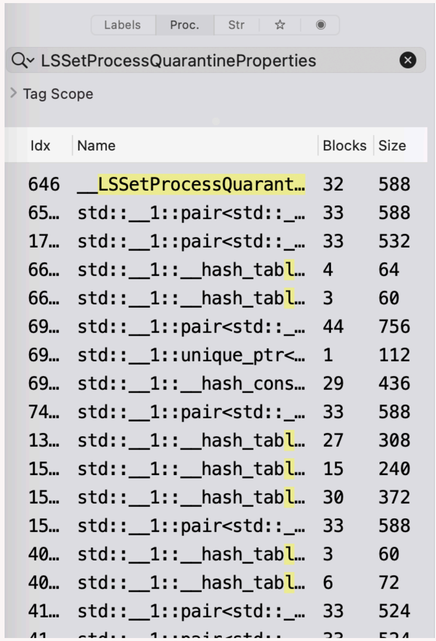
```
arthur — lldb --wait-for --attach-name Google Chrome ▸ Google Chrome — 119×22
(lldb) bt
* thread #1, queue = 'com.apple.main-thread', stop reason = breakpoint 1.1
  * frame #0: 0x0000000183de44c4 LaunchServices`_LSSetProcessQuarantineProperties
    frame #1: 0x0000000183de40e4 LaunchServices`_LSRegisterSelf + 468
    frame #2: 0x0000000183db45e4 LaunchServices`_LSApplicationCheckIn + 7948
    frame #3: 0x00000001890da8ac HIServices`_RegisterApplication + 5284
    frame #4: 0x00000001890d92bc HIServices`GetCurrentProcess + 36
    frame #5: 0x000000018d009958 HIToolbox`MenuBarInstance::GetAggregateUIMode(unsigned int*, unsigned int*) + 84
    frame #6: 0x000000018d0098c4 HIToolbox`MenuBarInstance::IsVisible() + 56
    frame #7: 0x0000000186babb44 AppKit`_NSInitializeAppContext + 108
    frame #8: 0x0000000186ba9ac0 AppKit`-[NSApplication init] + 404
    frame #9: 0x0000000186ba9760 AppKit`+[NSApplication sharedApplication] + 128
    frame #10: 0x000000011ac24fd4 Google Chrome Framework`___lldb_unnamed_symbol2657 + 515912
    frame #11: 0x000000011b53f004 Google Chrome Framework`___lldb_unnamed_symbol2693 + 70888
    frame #12: 0x000000011b53ede8 Google Chrome Framework`___lldb_unnamed_symbol2693 + 70348
    frame #13: 0x000000011b3be63c Google Chrome Framework`___lldb_unnamed_symbol2689 + 86840
    frame #14: 0x000000011a812d00 Google Chrome Framework`___lldb_unnamed_symbol2632 + 37596
    frame #15: 0x000000011a811dbc Google Chrome Framework`___lldb_unnamed_symbol2632 + 33688
    frame #16: 0x0000000118fc4ef8 Google Chrome Framework`ChromeMain + 688
    frame #17: 0x000000010239d55c Google Chrome`main + 196
    frame #18: 0x0000000018354fe50 dyld`start + 2544
(lldb)
```

lldb output with breakpoint set on “LSSetProcessQuarantineProperties” symbol

Investigation: Hopper Disassembler



LSSetProcessQuarantineProperties creates a struct that represents the running process

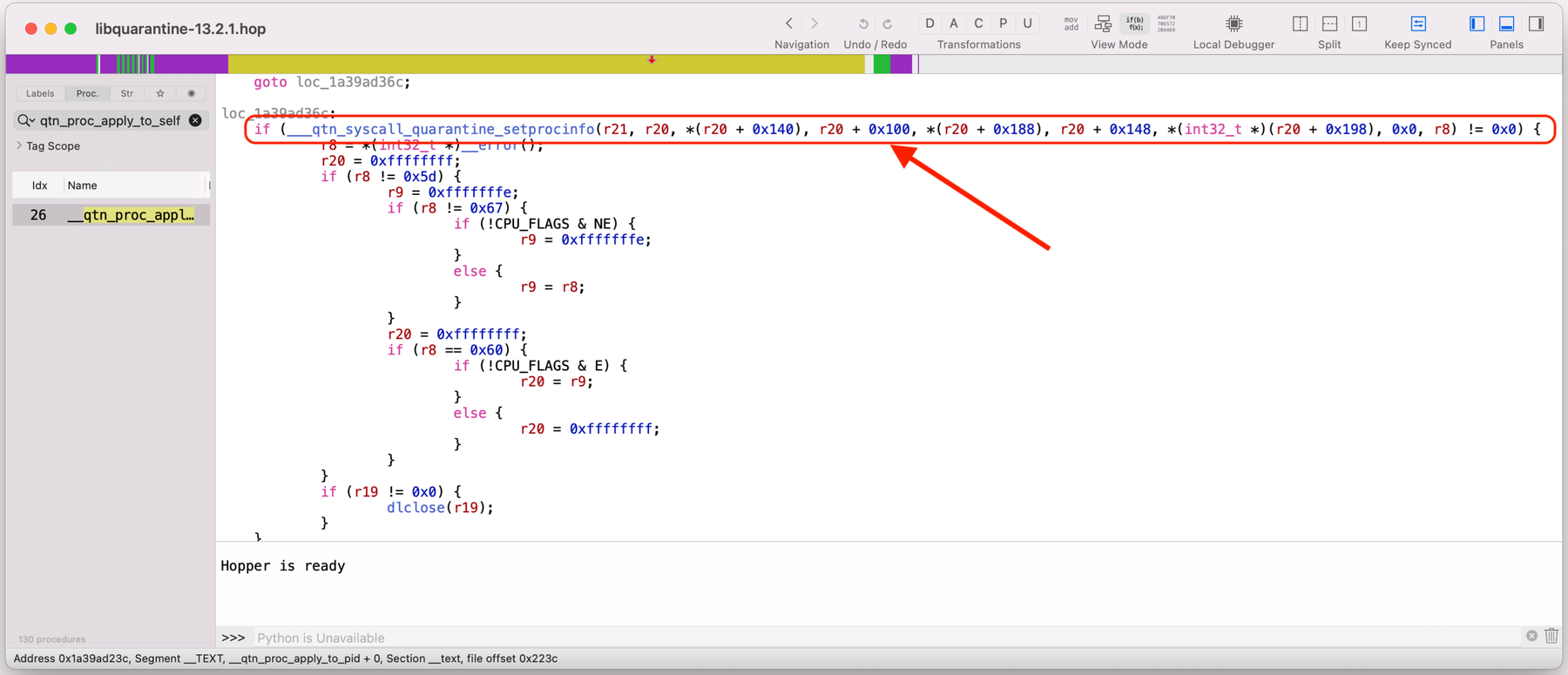




```
                }
            }
        }
        CFRelease(r19);
        r19 = _qtn_proc_apply_to_self();
        if (r20 != 0x0) {
            _qtn_proc_free();
        }
        if (r19 != 0x0) {
            r0 = __LSGetOSStatusFromPOSIXErrorCode(r19);
        }
        else {
            r0 = 0x0;
        }
    }
    else {
        r19 = _qtn_proc_apply_to_self();
        if (r19 == 0x0) {
            r0 = 0x0;
        }
        else {
            r0 = __LSGetOSStatusFromPOSIXErrorCode(r19);
        }
    }
    if (**0x1f99634d8 != **0x1f99634d8) {
        r0 = __stack_chk_fail();
    }
    return r0;
}
```

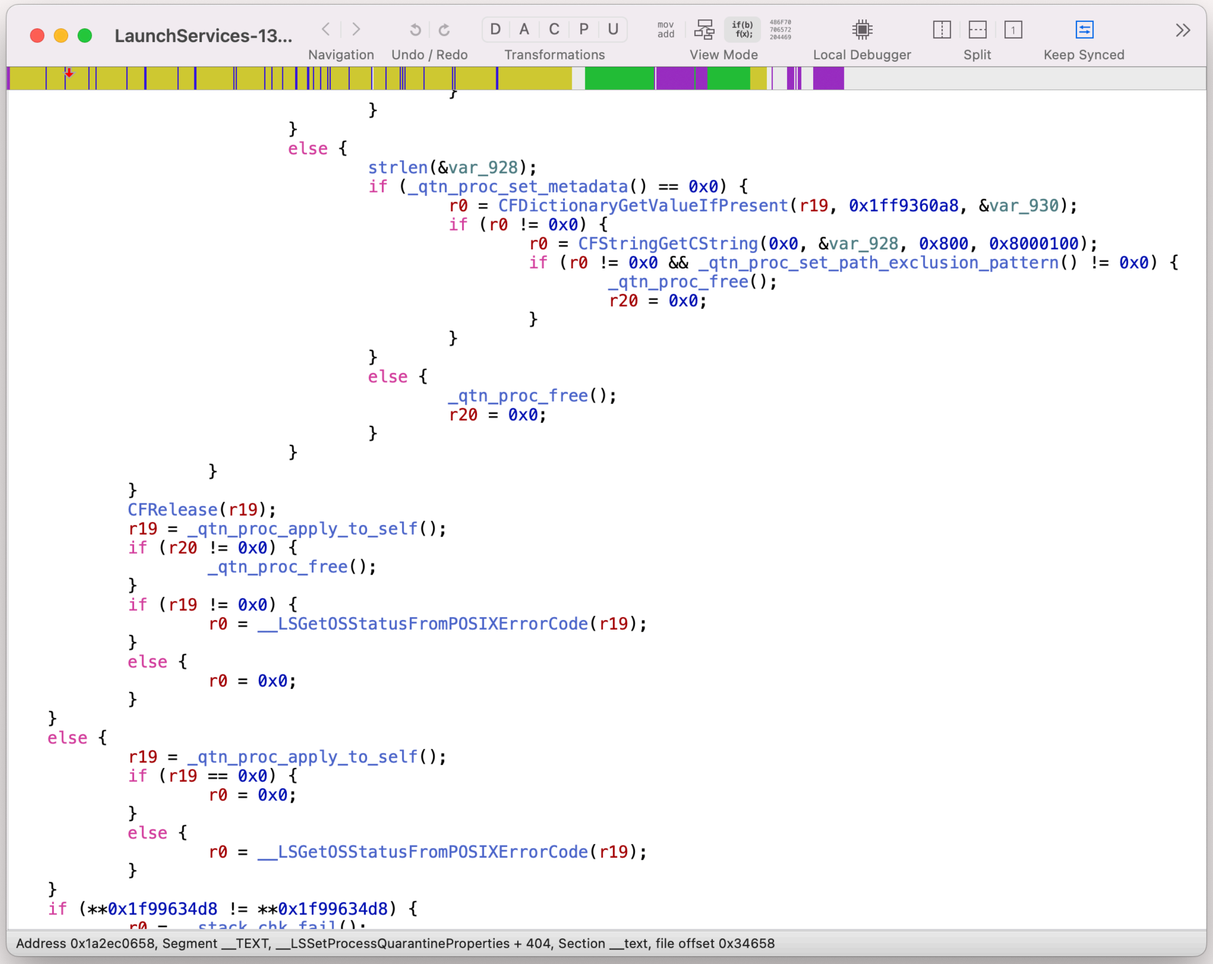
Calling into libquarantine.dylib to propagate collected metadata

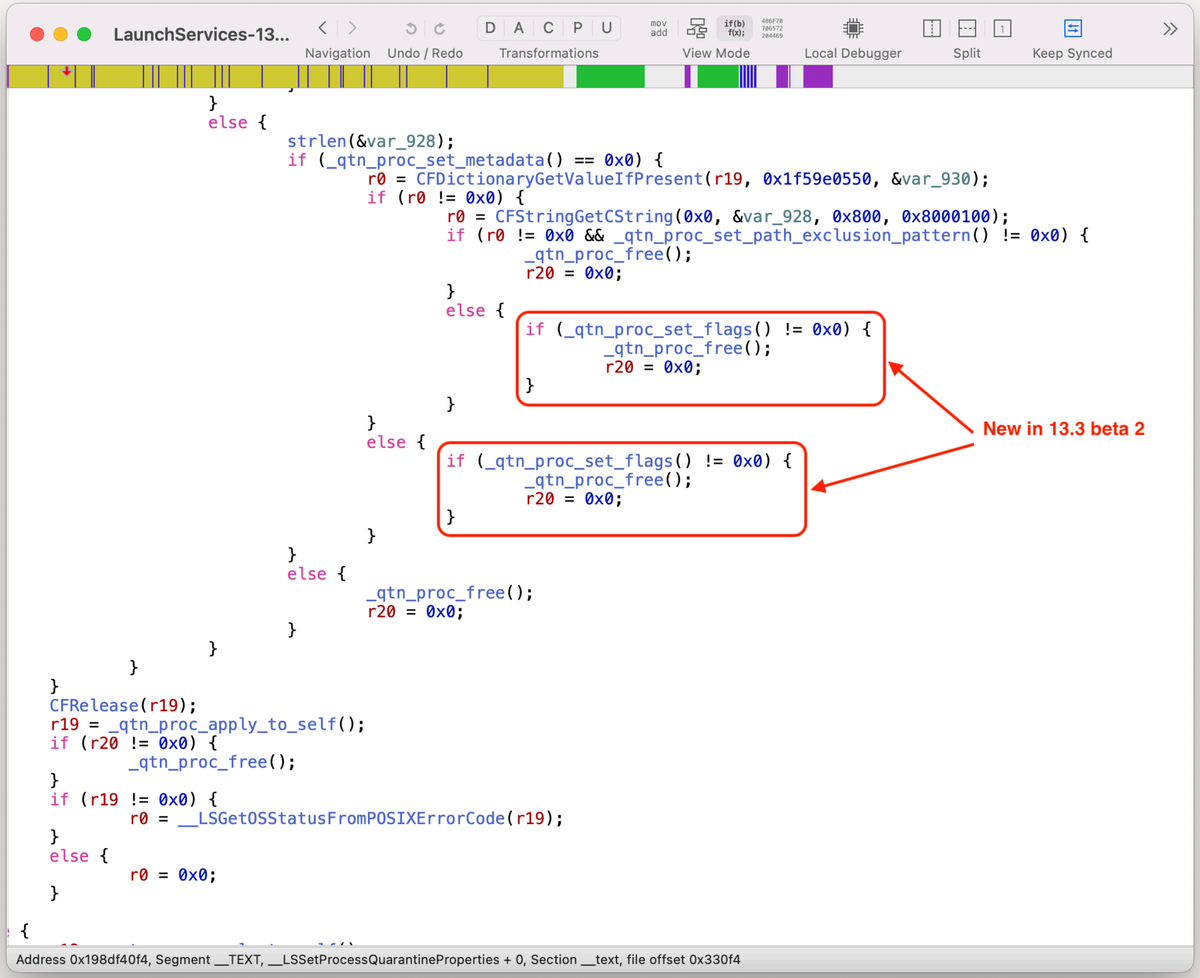
Investigation: Hopper Disassembler



"qtn_proc_apply_to_self" is a wrapper around "qtn_proc_apply_to_pid"
which invokes a system call passing all collected process information to the kernel

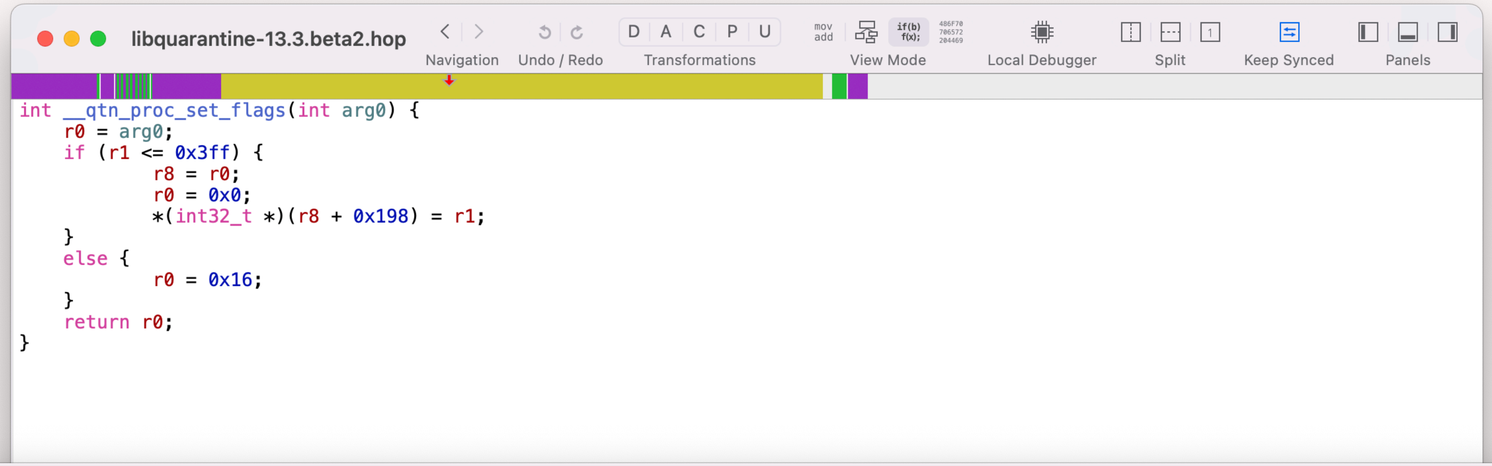
Investigation: Hopper Disassembler

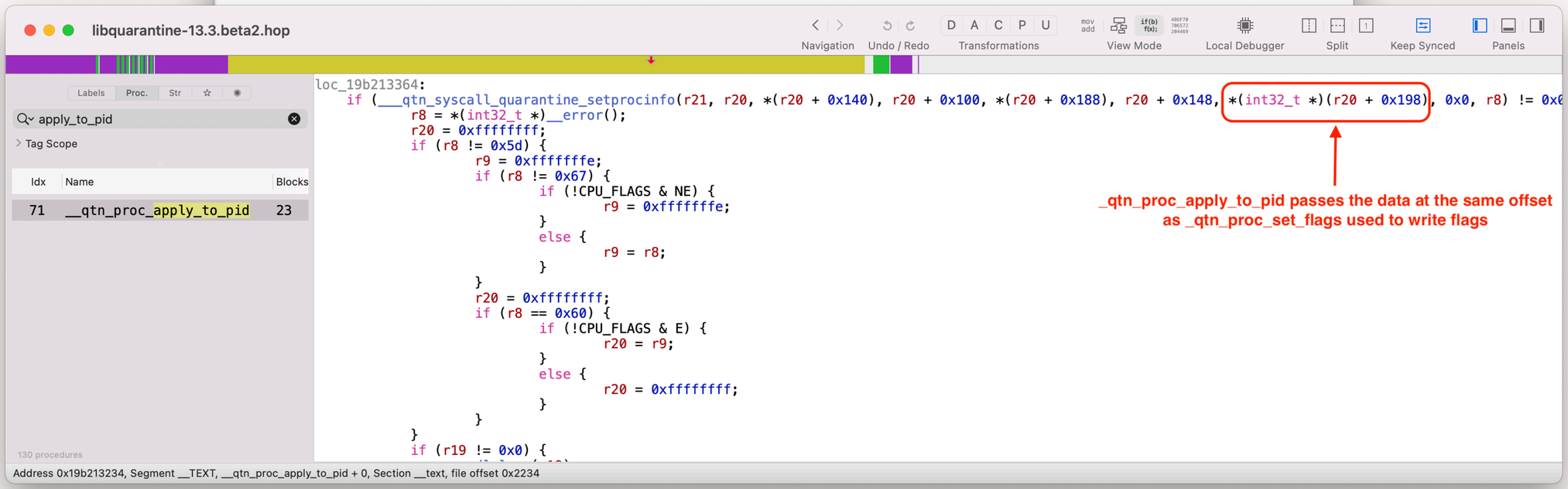




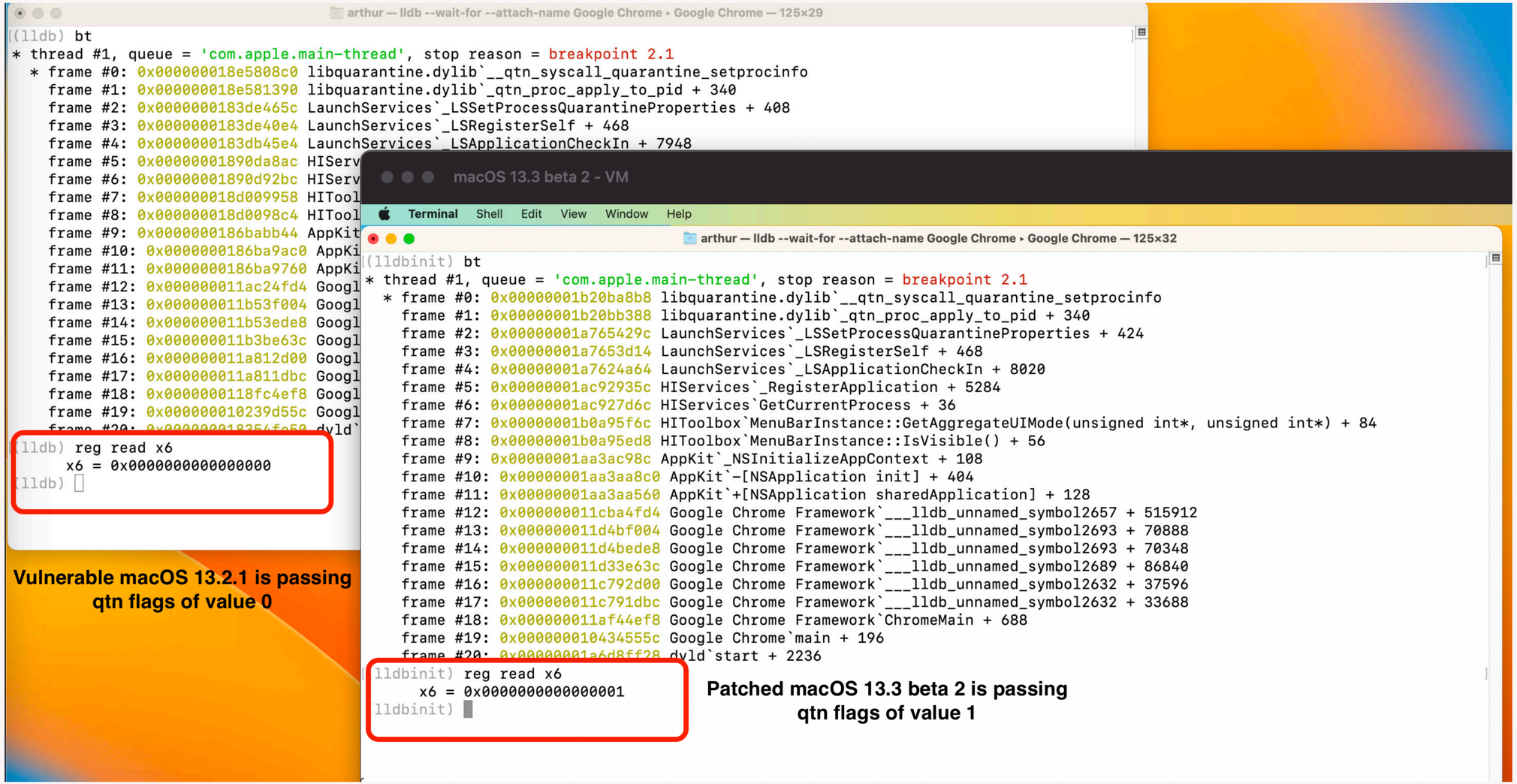
Diff of “LSSetProcessQuarantineProperties” function between 13.2.1 and 13.3 beta 2

Investigation: Hopper Disassembler





Investigation: LLDB



Difference in qtn flags value between vulnerable and patched version of macOS (13.2.1 vs. 13.3 beta 2)

Future research on the topic

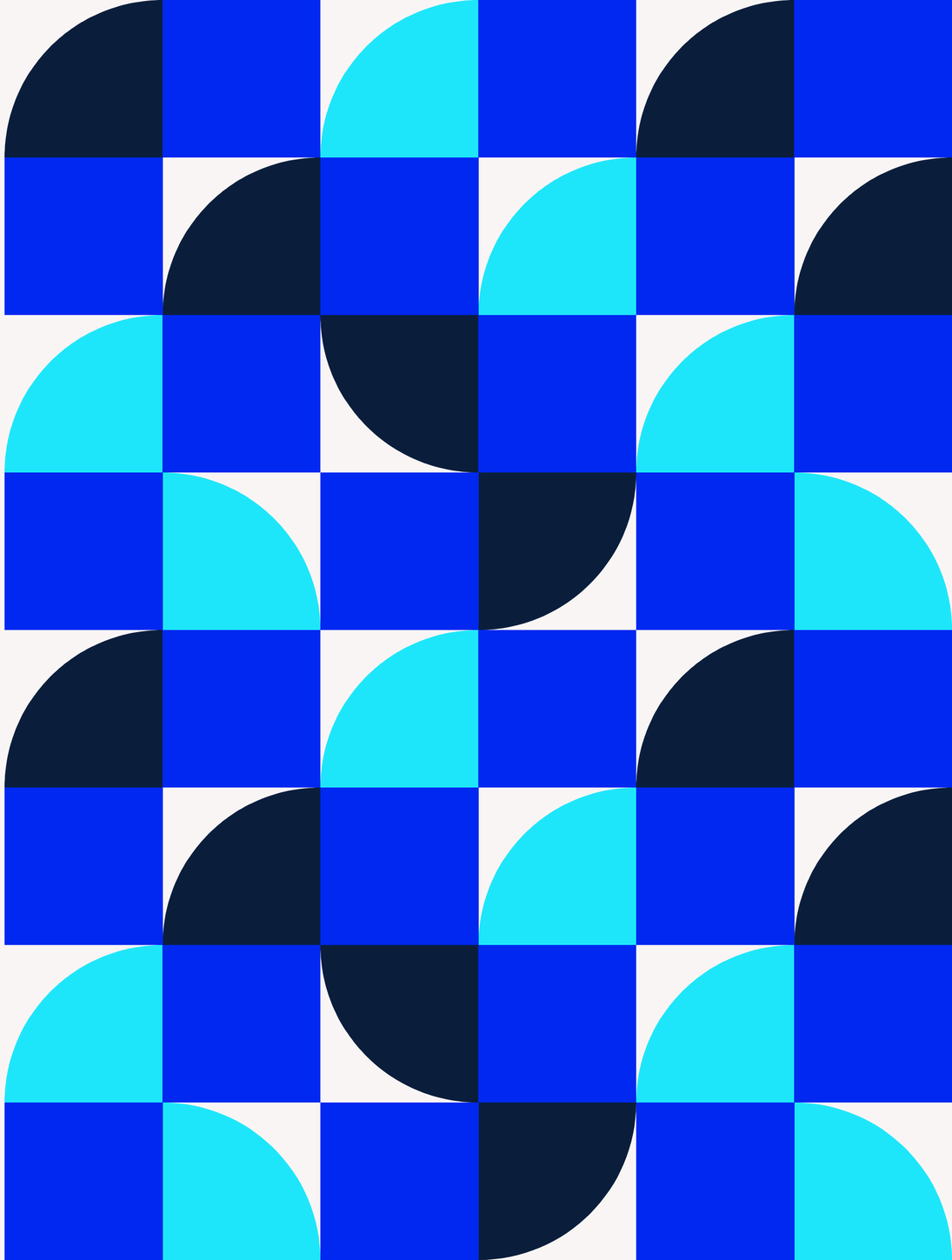
- The kernel side of the story still remains somewhat a mystery.
  - Attempts of live system debugging on latest macOS versions were so far unsuccessful.
  - Apple provided tooling (kdp-remote) is causing kernel panics and memory corruption after resume of a breakpoint.
- The vulnerability was reproduced when quarantine attribute was set on the app with LSFileQuarantineEnabled key in Info.plist.
  - Why was the vulnerability only seen in this case?
  - Is it the reason why Apple did not catch this in time?
- macOS Monterey was not affected by the reported issue.
  - What logic did the kernel have before Ventura?
  - Was it filling in the flag metadata passed on macOS Ventura with __qtn_proc_set_flags on its own?
  - How did it make the decision to set the quarantine attribute when LSFileQuarantineEnabled key is present?

F-Secure

CVE-2021-1810

A journey through archive extraction, quarantine attribute propagation and long file paths

Rasmus Sten



F-Secure

CVE-2021-1810

Archive Utility

Available for: macOS Big Sur

Impact: A malicious application may bypass Gatekeeper checks

Description: A logic issue was addressed with improved state management.

CVE-2021-1810: Rasmus Sten (@pajp) of F-Secure

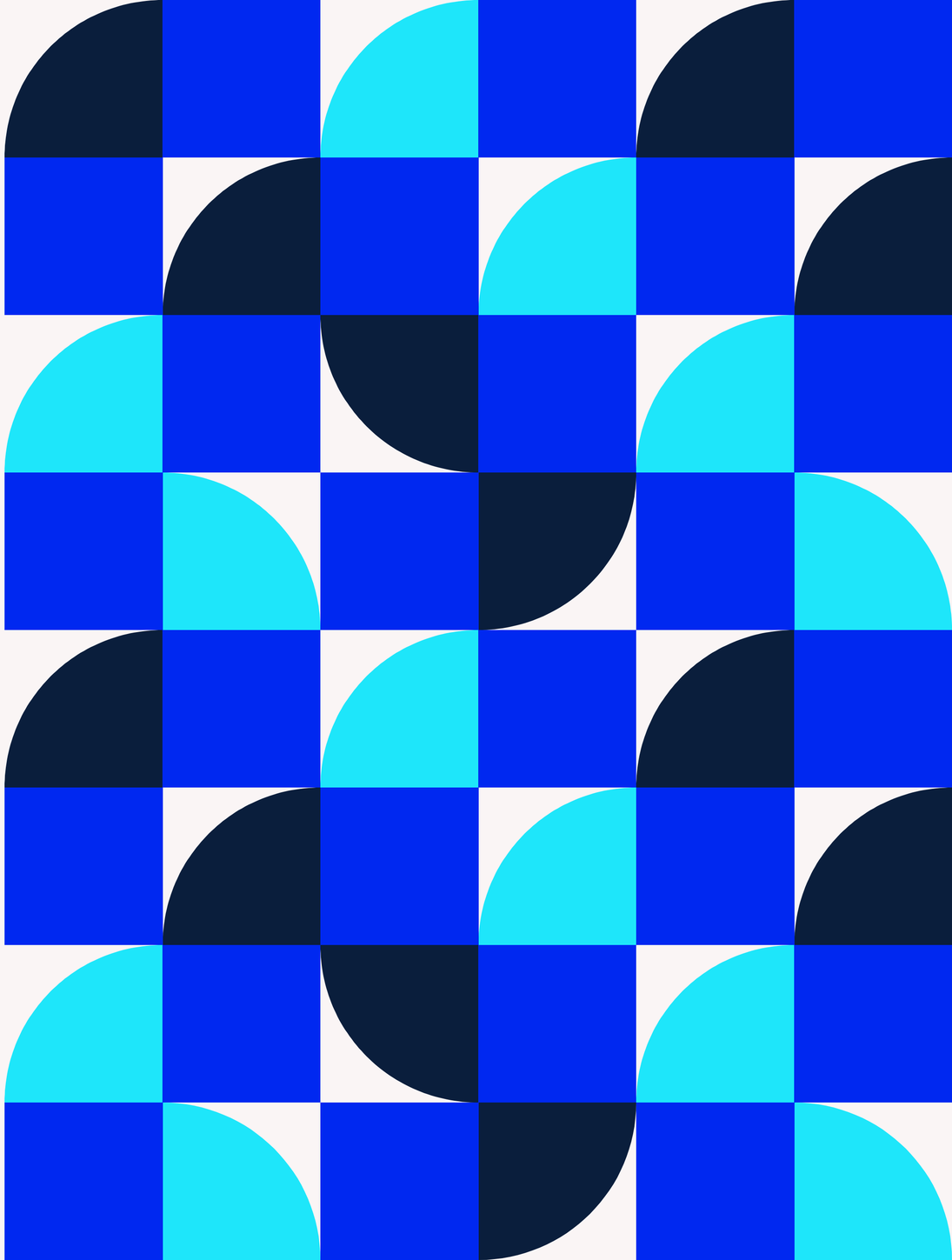
Archive Utility

Available for: macOS Catalina

Impact: A malicious application may bypass Gatekeeper checks

Description: A logic issue was addressed with improved state management.

CVE-2021-1810: Rasmus Sten (@pajp) of F-Secure



Special shout out to a related talk from last year's OBTS:

"Bombastically Abominating Bomshellz" - OBTS v5.0

Discovery process

- Customer complained about UI bug related to long file names
- Started to explore downloading zip files with deep directory hierarchies
  - File/folder name limit: 255 bytes. PATH_MAX = 1024 bytes
- Noticed the deep end was **missing the com.apple.quarantine extended attribute**
  - (The quarantine attribute is of course Very Important™ to Gatekeeper, but also important to our product.)
- At first it looked like the cut-off was PATH_MAX - which wouldn't be exploitable because macOS refuses to execute files with path names >PATH_MAX, but…


Downloads — -zsh — 194×69
rasmus@catalina-beta-vm Downloads % echo -n /Users/rasmus/Downloads/yxxxxxxxxxx1/yxxxxxxxxxx2/yxxxxxxxxxx3/yxxxxxxxxxx4/yxxxxxxxxxx5/yxxxxxxxxxx6/yxxxxxxxxxx7/yxxxxxxxxxx8/yxxxxxxxxxx9/
yxxxxxxxxxx10/yxxxxxxxxxx11/yxxxxxxxxxx12/yxxxxxxxxxx13/yxxxxxxxxxx14/yxxxxxxxxxx15/yxxxxxxxxxx16/yxxxxxxxxxx17/yxxxxxxxxxx18/yxxxxxxxxxx19/yxxxxxxxxxx20/yxxxxxxxxxx21/yxxxxxxxxxx22
/yxxxxxxxxxx23/yxxxxxxxxxx24/yxxxxxxxxxx25/yxxxxxxxxxx26/yxxxxxxxxxx27/yxxxxxxxxxx28/yxxxxxxxxxx29/yxxxxxxxxxx30/yxxxxxxxxxx31/yxxxxxxxxxx32/yxxxxxxxxxx33/yxxxxxxxxxx34/yxxxxxxxxxx3
5/yxxxxxxxxxx36/yxxxxxxxxxx37/yxxxxxxxxxx38/yxxxxxxxxxx39/yxxxxxxxxxx40/yxxxxxxxxxx41/yxxxxxxxxxx42/yxxxxxxxxxx43/yxxxxxxxxxx44/yxxxxxxxxxx45/yxxxxxxxxxx46/yxxxxxxxxxx47/yxxxxxxxxxx
48/yxxxxxxxxxx49/yxxxxxxxxxx50/yxxxxxxxxxx51/yxxxxxxxxxx52/yxxxxxxxxxx53/yxxxxxxxxxx54/yxxxxxxxxxx55/yxxxxxxxxxx56/yxxxxxxxxxx57/yxxxxxxxxxx58/yxxxxxxxxxx59/dummyfile|wc -c
909
rasmus@catalina-beta-vm Downloads % ls -l@ /Users/rasmus/Downloads/yxxxxxxxxxx1/yxxxxxxxxxx2/yxxxxxxxxxx3/yxxxxxxxxxx4/yxxxxxxxxxx5/yxxxxxxxxxx6/yxxxxxxxxxx7/yxxxxxxxxxx8/yxxxxxxxxxx9/y
xxxxxxxxxx10/yxxxxxxxxxx11/yxxxxxxxxxx12/yxxxxxxxxxx13/yxxxxxxxxxx14/yxxxxxxxxxx15/yxxxxxxxxxx16/yxxxxxxxxxx17/yxxxxxxxxxx18/yxxxxxxxxxx19/yxxxxxxxxxx20/yxxxxxxxxxx21/yxxxxxxxxxx22/
yxxxxxxxxxx23/yxxxxxxxxxx24/yxxxxxxxxxx25/yxxxxxxxxxx26/yxxxxxxxxxx27/yxxxxxxxxxx28/yxxxxxxxxxx29/yxxxxxxxxxx30/yxxxxxxxxxx31/yxxxxxxxxxx32/yxxxxxxxxxx33/yxxxxxxxxxx34/yxxxxxxxxxx35
/yxxxxxxxxxx36/yxxxxxxxxxx37/yxxxxxxxxxx38/yxxxxxxxxxx39/yxxxxxxxxxx40/yxxxxxxxxxx41/yxxxxxxxxxx42/yxxxxxxxxxx43/yxxxxxxxxxx44/yxxxxxxxxxx45/yxxxxxxxxxx46/yxxxxxxxxxx47/yxxxxxxxxxx4
8/yxxxxxxxxxx49/yxxxxxxxxxx50/yxxxxxxxxxx51/yxxxxxxxxxx52/yxxxxxxxxxx53/yxxxxxxxxxx54/yxxxxxxxxxx55/yxxxxxxxxxx56/yxxxxxxxxxx57/yxxxxxxxxxx58/yxxxxxxxxxx59/dummyfile
-rw-r--r-- 1 rasmus staff 0 May 6 11:19 /Users/rasmus/Downloads/yxxxxxxxxxx1/yxxxxxxxxxx2/yxxxxxxxxxx3/yxxxxxxxxxx4/yxxxxxxxxxx5/yxxxxxxxxxx6/yxxxxxxxxxx7/yxxxxxxxxxx8/yxxxxxxxxxx9/
yxxxxxxxxxx10/yxxxxxxxxxx11/yxxxxxxxxxx12/yxxxxxxxxxx13/yxxxxxxxxxx14/yxxxxxxxxxx15/yxxxxxxxxxx16/yxxxxxxxxxx17/yxxxxxxxxxx18/yxxxxxxxxxx19/yxxxxxxxxxx20/yxxxxxxxxxx21/yxxxxxxxxxx22
/yxxxxxxxxxx23/yxxxxxxxxxx24/yxxxxxxxxxx25/yxxxxxxxxxx26/yxxxxxxxxxx27/yxxxxxxxxxx28/yxxxxxxxxxx29/yxxxxxxxxxx30/yxxxxxxxxxx31/yxxxxxxxxxx32/yxxxxxxxxxx33/yxxxxxxxxxx34/yxxxxxxxxxx3
5/yxxxxxxxxxx36/yxxxxxxxxxx37/yxxxxxxxxxx38/yxxxxxxxxxx39/yxxxxxxxxxx40/yxxxxxxxxxx41/yxxxxxxxxxx42/yxxxxxxxxxx43/yxxxxxxxxxx44/yxxxxxxxxxx45/yxxxxxxxxxx46/yxxxxxxxxxx47/yxxxxxxxxxx
48/yxxxxxxxxxx49/yxxxxxxxxxx50/yxxxxxxxxxx51/yxxxxxxxxxx52/yxxxxxxxxxx53/yxxxxxxxxxx54/yxxxxxxxxxx55/yxxxxxxxxxx56/yxxxxxxxxxx57/yxxxxxxxxxx58/dummyfile
rasmus@catalina-beta-vm Downloads % ls -l@ /Users/rasmus/Downloads/yxxxxxxxxxx1/yxxxxxxxxxx2/yxxxxxxxxxx3/yxxxxxxxxxx4/yxxxxxxxxxx5/yxxxxxxxxxx6/yxxxxxxxxxx7/yxxxxxxxxxx8/yxxxxxxxxxx9/y
xxxxxxxxxx10/yxxxxxxxxxx11/yxxxxxxxxxx12/yxxxxxxxxxx13/yxxxxxxxxxx14/yxxxxxxxxxx15/yxxxxxxxxxx16/yxxxxxxxxxx17/yxxxxxxxxxx18/yxxxxxxxxxx19/yxxxxxxxxxx20/yxxxxxxxxxx21/yxxxxxxxxxx22/
yxxxxxxxxxx23/yxxxxxxxxxx24/yxxxxxxxxxx25/yxxxxxxxxxx26/yxxxxxxxxxx27/yxxxxxxxxxx28/yxxxxxxxxxx29/yxxxxxxxxxx30/yxxxxxxxxxx31/yxxxxxxxxxx32/yxxxxxxxxxx33/yxxxxxxxxxx34/yxxxxxxxxxx35
/yxxxxxxxxxx36/yxxxxxxxxxx37/yxxxxxxxxxx38/yxxxxxxxxxx39/yxxxxxxxxxx40/yxxxxxxxxxx41/yxxxxxxxxxx42/yxxxxxxxxxx43/yxxxxxxxxxx44/yxxxxxxxxxx45/yxxxxxxxxxx46/yxxxxxxxxxx47/yxxxxxxxxxx4
8/yxxxxxxxxxx49/yxxxxxxxxxx50/yxxxxxxxxxx51/yxxxxxxxxxx52/yxxxxxxxxxx53/yxxxxxxxxxx54/yxxxxxxxxxx55/yxxxxxxxxxx56/yxxxxxxxxxx57/yxxxxxxxxxx58/dummyfile
-rw-r--r--@ 1 rasmus staff 0 May 6 11:19 /Users/rasmus/Downloads/yxxxxxxxxxx1/yxxxxxxxxxx2/yxxxxxxxxxx3/yxxxxxxxxxx4/yxxxxxxxxxx5/yxxxxxxxxxx6/yxxxxxxxxxx7/yxxxxxxxxxx8/yxxxxxxxxxx9/
yxxxxxxxxxx10/yxxxxxxxxxx11/yxxxxxxxxxx12/yxxxxxxxxxx13/yxxxxxxxxxx14/yxxxxxxxxxx15/yxxxxxxxxxx16/yxxxxxxxxxx17/yxxxxxxxxxx18/yxxxxxxxxxx19/yxxxxxxxxxx20/yxxxxxxxxxx21/yxxxxxxxxxx22
/yxxxxxxxxxx23/yxxxxxxxxxx24/yxxxxxxxxxx25/yxxxxxxxxxx26/yxxxxxxxxxx27/yxxxxxxxxxx28/yxxxxxxxxxx29/yxxxxxxxxxx30/yxxxxxxxxxx31/yxxxxxxxxxx32/yxxxxxxxxxx33/yxxxxxxxxxx34/yxxxxxxxxxx3
5/yxxxxxxxxxx36/yxxxxxxxxxx37/yxxxxxxxxxx38/yxxxxxxxxxx39/yxxxxxxxxxx40/yxxxxxxxxxx41/yxxxxxxxxxx42/yxxxxxxxxxx43/yxxxxxxxxxx44/yxxxxxxxxxx45/yxxxxxxxxxx46/yxxxxxxxxxx47/yxxxxxxxxxx
48/yxxxxxxxxxx49/yxxxxxxxxxx50/yxxxxxxxxxx51/yxxxxxxxxxx52/yxxxxxxxxxx53/yxxxxxxxxxx54/yxxxxxxxxxx55/yxxxxxxxxxx56/yxxxxxxxxxx57/yxxxxxxxxxx58/dummyfile
com.apple.quarantine 57
rasmus@catalina-beta-vm Downloads % echo -n /Users/rasmus/Downloads/yxxxxxxxxxx1/yxxxxxxxxxx2/yxxxxxxxxxx3/yxxxxxxxxxx4/yxxxxxxxxxx5/yxxxxxxxxxx6/yxxxxxxxxxx7/yxxxxxxxxxx8/yxxxxxxxxxx9/
yxxxxxxxxxx10/yxxxxxxxxxx11/yxxxxxxxxxx12/yxxxxxxxxxx13/yxxxxxxxxxx14/yxxxxxxxxxx15/yxxxxxxxxxx16/yxxxxxxxxxx17/yxxxxxxxxxx18/yxxxxxxxxxx19/yxxxxxxxxxx20/yxxxxxxxxxx21/yxxxxxxxxxx22
/yxxxxxxxxxx23/yxxxxxxxxxx24/yxxxxxxxxxx25/yxxxxxxxxxx26/yxxxxxxxxxx27/yxxxxxxxxxx28/yxxxxxxxxxx29/yxxxxxxxxxx30/yxxxxxxxxxx31/yxxxxxxxxxx32/yxxxxxxxxxx33/yxxxxxxxxxx34/yxxxxxxxxxx3
5/yxxxxxxxxxx36/yxxxxxxxxxx37/yxxxxxxxxxx38/yxxxxxxxxxx39/yxxxxxxxxxx40/yxxxxxxxxxx41/yxxxxxxxxxx42/yxxxxxxxxxx43/yxxxxxxxxxx44/yxxxxxxxxxx45/yxxxxxxxxxx46/yxxxxxxxxxx47/yxxxxxxxxxx
48/yxxxxxxxxxx49/yxxxxxxxxxx50/yxxxxxxxxxx51/yxxxxxxxxxx52/yxxxxxxxxxx53/yxxxxxxxxxx54/yxxxxxxxxxx55/yxxxxxxxxxx56/yxxxxxxxxxx57/yxxxxxxxxxx58/dummyfile|wc -c
894
rasmus@catalina-beta-vm Downloads %

The sweet spot

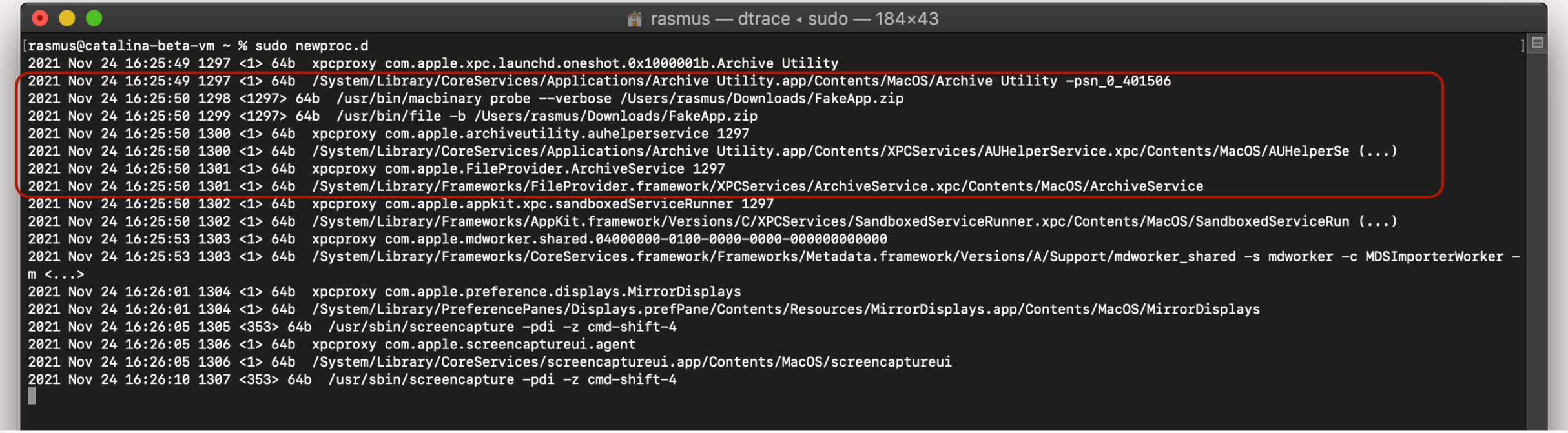
- Turns out that the point at which Archive Utility fails to set the quarantine attribute is not actually PATH_MAX but (PATH_MAX - (some number))
- Experimentally I see that it's somewhere between 894 and 909
- This means that we can drop an executable with a path name is:
  - Short enough to allow execution by macOS
  - Long enough to trigger the Archive Utility bug
- Placing an unsigned command-line executable with a path name in the sweet spot → we have a Gateekeeper bypass!
  - Although a bit awkward to deploy…

Turning it into a PoC

- By default Safari will unzip files using its own built-in unarchive tool
- It turns out this tool does *not* have the same issue
- However it *also* will refuse to unpack archives with paths >PATH_MAX - with no error message to the user
- To sum it all up, we can make an archive that has:
  - A long, “.hidden”, path that will prevent Safari unpacking
  - An app bundle in the “sweet spot” that gets written without quarantine xattr, placed in a “.hidden” folder
  - A symlink at the root of the zip file pointing the app bundle

Root cause analysis

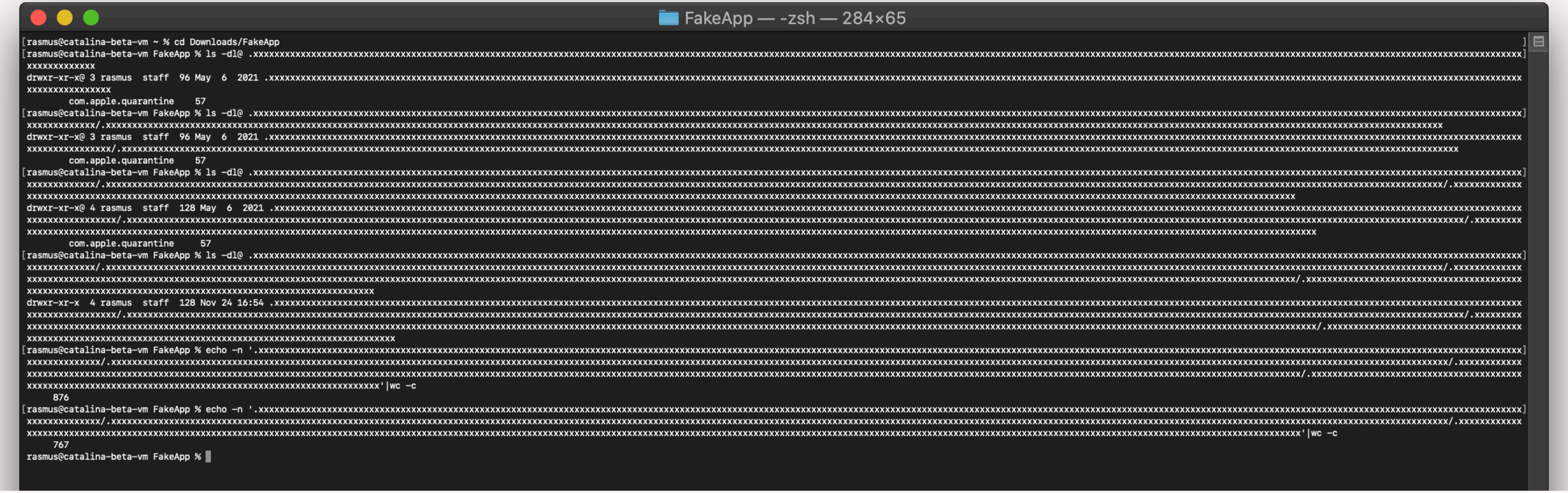
- What processes are involved when unpacking something with Archive Utility?
  - ”newproc.d” - DTrace script which prints process launch events - in modern macOS you can use “eslogger exec”
    - DTrace disabled by default, need to be enabled from Recovery mode using ”csrutil”
- Caution! Disabling SIP entirely caused “fixed” the vulnerability! No, I don’t know why. “csrutil --enable --without-dtrace" works



rasmus — fs_usage ◂ sudo — 284×65

```
16:54:41.625356  lstat64                                           /private                                                                                                                                                                  0.000006   ArchiveService.42091
16:54:41.625359  pthread_chdir                                     /private                                                                                                                                                                  0.000003   ArchiveService.42091
16:54:41.625361  lstat64                                           var                                                                                                                                                                       0.000002   ArchiveService.42091
16:54:41.625362  pthread_chdir                                     var                                                                                                                                                                       0.000001   ArchiveService.42091
16:54:41.625364  lstat64                                           folders                                                                                                                                                                   0.000002   ArchiveService.42091
16:54:41.625365  pthread_chdir                                     folders                                                                                                                                                                   0.000001   ArchiveService.42091
16:54:41.625366  lstat64                                           3d                                                                                                                                                                        0.000002   ArchiveService.42091
16:54:41.625368  pthread_chdir                                     3d                                                                                                                                                                        0.000001   ArchiveService.42091
16:54:41.625369  lstat64                                           4gzq8yw97cz35_55yqpv3pyh0000gn                                                                                                                                            0.000002   ArchiveService.42091
16:54:41.625371  pthread_chdir                                     4gzq8yw97cz35_55yqpv3pyh0000gn                                                                                                                                            0.000001   ArchiveService.42091
16:54:41.625372  lstat64                                           T                                                                                                                                                                         0.000002   ArchiveService.42091
16:54:41.625373  pthread_chdir                                     T                                                                                                                                                                         0.000001   ArchiveService.42091
16:54:41.625376  lstat64                                           com.apple.fileprovider.ArchiveService                                                                                                                                     0.000002   ArchiveService.42091
16:54:41.625377  pthread_chdir                                     com.apple.fileprovider.ArchiveService                                                                                                                                     0.000001   ArchiveService.42091
16:54:41.625379  lstat64                                           TemporaryItems                                                                                                                                                            0.000002   ArchiveService.42091
16:54:41.625380  pthread_chdir                                     TemporaryItems                                                                                                                                                            0.000001   ArchiveService.42091
16:54:41.625382  lstat64                                           (A Document Being Saved By ArchiveService)                                                                                                                                0.000002   ArchiveService.42091
16:54:41.625383  pthread_chdir                                     (A Document Being Saved By ArchiveService)                                                                                                                                0.000001   ArchiveService.42091
16:54:41.625386  lstat64                                           xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx    0.000003   ArchiveService.42091
16:54:41.625388  pthread_chdir                                     xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx    0.000002   ArchiveService.42091
16:54:41.625391  lstat64                                           xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx    0.000003   ArchiveService.42091
16:54:41.625393  pthread_chdir                                     xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx    0.000002   ArchiveService.42091
16:54:41.625396  lstat64                                           xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx    0.000003   ArchiveService.42091
16:54:41.625398  pthread_chdir                                     xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx    0.000002   ArchiveService.42091
16:54:41.625401  lstat64                                           .xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx                                                      0.000002   ArchiveService.42091
16:54:41.625402  pthread_chdir                                     .xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx                                                      0.000002   ArchiveService.42091
16:54:41.625404  lstat64                                           FakeApp.app                                                                                                                                                               0.000002   ArchiveService.42091
16:54:41.625405  pthread_chdir                                     FakeApp.app                                                                                                                                                               0.000001   ArchiveService.42091
16:54:41.625407  lstat64                                           Contents                                                                                                                                                                  0.000002   ArchiveService.42091
16:54:41.625408  pthread_chdir                                     Contents                                                                                                                                                                  0.000001   ArchiveService.42091
16:54:41.625410  lstat64                                           MacOS                                                                                                                                                                     0.000002   ArchiveService.42091
16:54:41.625412  pthread_chdir                                     MacOS                                                                                                                                                                     0.000002   ArchiveService.42091
16:54:41.625417  lstat64                       [   2]              HelloWorld                                                                                                                                                                0.000005   ArchiveService.42091
16:54:41.625419  close                F=4                                                                                                                                                                                                    0.000002   ArchiveService.42091
16:54:41.625428  open                 F=4           (R_________X)  .                                                                                                                                                                         0.000009   ArchiveService.42091
16:54:41.625438  stat64                                            xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx    0.000009   ArchiveService.42091
16:54:41.625446  chdir                                             xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx    0.000007   ArchiveService.42091
16:54:41.625525  open                 F=5           (_WC__E_____X)  .xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx/FakeApp.app/Contents/MacOS/HelloWorld          0.000080   ArchiveService.42091
16:54:41.625562  close                F=4                                                                                                                                                                                                    0.000002   ArchiveService.42091
16:54:41.626310  close                F=5                                                                                                                                                                                                    0.000158   ArchiveService.42091
16:54:41.626375  open                 F=4           (R_________X)  .                                                                                                                                                                         0.000019   ArchiveService.42091
16:54:41.626386  lstat64                                           /private                                                                                                                                                                  0.000010   ArchiveService.42091
16:54:41.626390  pthread_chdir                                     /private                                                                                                                                                                  0.000003   ArchiveService.42091
16:54:41.626392  lstat64                                           var                                                                                                                                                                       0.000002   ArchiveService.42091
16:54:41.626393  pthread_chdir                                     var                                                                                                                                                                       0.000001   ArchiveService.42091
16:54:41.626395  lstat64                                           folders                                                                                                                                                                   0.000002   ArchiveService.42091
16:54:41.626396  pthread_chdir                                     folders                                                                                                                                                                   0.000001   ArchiveService.42091
16:54:41.626398  lstat64                                           3d                                                                                                                                                                        0.000002   ArchiveService.42091
16:54:41.626399  pthread_chdir                                     3d                                                                                                                                                                        0.000001   ArchiveService.42091
16:54:41.626402  lstat64                                           4gzq8yw97cz35_55yqpv3pyh0000gn                                                                                                                                            0.000002   ArchiveService.42091
16:54:41.626403  pthread_chdir                                     4gzq8yw97cz35_55yqpv3pyh0000gn                                                                                                                                            0.000001   ArchiveService.42091
16:54:41.626405  lstat64                                           T                                                                                                                                                                         0.000002   ArchiveService.42091
16:54:41.626406  pthread_chdir                                     T                                                                                                                                                                         0.000001   ArchiveService.42091
16:54:41.626408  lstat64                                           com.apple.fileprovider.ArchiveService                                                                                                                                     0.000003   ArchiveService.42091
16:54:41.626409  pthread_chdir                                     com.apple.fileprovider.ArchiveService                                                                                                                                     0.000001   ArchiveService.42091
16:54:41.626411  lstat64                                           TemporaryItems                                                                                                                                                            0.000002   ArchiveService.42091
16:54:41.626412  pthread_chdir                                     TemporaryItems                                                                                                                                                            0.000001   ArchiveService.42091
16:54:41.626415  lstat64                                           (A Document Being Saved By ArchiveService)                                                                                                                                0.000003   ArchiveService.42091
16:54:41.626416  pthread_chdir                                     (A Document Being Saved By ArchiveService)                                                                                                                                0.000001   ArchiveService.42091
16:54:41.626419  lstat64                                           xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx    0.000003   ArchiveService.42091
16:54:41.626421  pthread_chdir                                     xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx    0.000002   ArchiveService.42091
16:54:41.626425  lstat64                                           xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx    0.000003   ArchiveService.42091
16:54:41.626427  pthread_chdir                                     xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx    0.000002   ArchiveService.42091
16:54:41.626430  lstat64                                           xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx    0.000003   ArchiveService.42091
16:54:41.626432  pthread_chdir                                     xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx    0.000002   ArchiveService.42091
```

fs_usage(1) output during archive extraction



- 876 + 152 = 1028 -> no quarantine attribute
- 767 + 152 = 919 -> quarantine attribute

Digging deeper with DTrace

- Let's list all Dtrace probes with "xattr" in them!
  - Oops, that was a lot, but a lot of them are called "setxattr"/"getxattr", let's narrow it down to "setxattr"

```
rasmus@catalina-beta-vm ~ % cat setxattr.d
::*setxattr*:entry {
    stack();
    ustack();
}
```

dtrace script that prints kernel- and user space stacks

```
rasmus@catalina-beta-vm ~ % sudo dtrace -l | grep setxattr
  630     syscall                                          setxattr entry
  631     syscall                                          setxattr return
  632     syscall                                         fsetxattr entry
  633     syscall                                         fsetxattr return
 2201      fsinfo       mach_kernel                    VNOP_SETXATTR setxattr
132903         fbt com.apple.filesystems.apfs               apfs_vnop_setxattr entry
132904         fbt com.apple.filesystems.apfs               apfs_vnop_setxattr return
132945         fbt com.apple.filesystems.apfs      apfs_setxattr_as_namedstream entry
132946         fbt com.apple.filesystems.apfs      apfs_setxattr_as_namedstream return
132947         fbt com.apple.filesystems.apfs            apfs_setxattr_internal entry
132948         fbt com.apple.filesystems.apfs            apfs_setxattr_internal return
134038         fbt com.apple.filesystems.apfs           apfs_fake_vnop_setxattr entry
134039         fbt com.apple.filesystems.apfs           apfs_fake_vnop_setxattr return
147971         fbt com.apple.filesystems.hfs.kext         hfs_exchangedata_setxattr entry
147972         fbt com.apple.filesystems.hfs.kext         hfs_exchangedata_setxattr return
148171         fbt com.apple.filesystems.hfs.kext                hfs_vnop_setxattr entry
148172         fbt com.apple.filesystems.hfs.kext                hfs_vnop_setxattr return
148173         fbt com.apple.filesystems.hfs.kext             hfs_setxattr_internal entry
148174         fbt com.apple.filesystems.hfs.kext             hfs_setxattr_internal return
192670         fbt       mach_kernel                 nfs4_vnop_setxattr entry
192671         fbt       mach_kernel                 nfs4_vnop_setxattr return
193498         fbt       mach_kernel                fpnfs_vnop_setxattr entry
193499         fbt       mach_kernel                fpnfs_vnop_setxattr return
194947         fbt       mach_kernel                          setxattr entry
194948         fbt       mach_kernel                          setxattr return
194949         fbt       mach_kernel                         fsetxattr entry
194950         fbt       mach_kernel                         fsetxattr return
195169         fbt       mach_kernel                        vn_setxattr entry
195170         fbt       mach_kernel                        vn_setxattr return
214647         fbt       mach_kernel                  mac_vnop_setxattr entry
214648         fbt       mach_kernel                  mac_vnop_setxattr return
214875         fbt       mach_kernel                  mac_file_setxattr entry
214876         fbt       mach_kernel                  mac_file_setxattr return
rasmus@catalina-beta-vm ~ %
```

```
1 132903          apfs_vnop_setxattr:entry
              kernel`VNOP_SETXATTR+0x59
              kernel`mac_vnop_setxattr+0x105
              Quarantine`quarantine_set_ea+0x5d
              Quarantine`syscall_quarantine_setinfo_common+0x5e2
              Quarantine`syscall_quarantine_setinfo_path+0xd4
              kernel`__mac_syscall+0xee
              kernel`unix_syscall64+0x287
              kernel`hndl_unix_scall64+0x16

              libsystem_kernel.dylib`__mac_syscall+0xa
              libquarantine.dylib`_qtn_file_apply_to_path+0x6
              Archive Utility`0x0000000[illegible]
              Archive Utility`0x000000010ffa71ef+0x244
              Foundation`__NSThread__start__+0x428
              libsystem_pthread.dylib`_pthread_start+0x94
              libsystem_pthread.dylib`thread_start+0xf
```

list of dtrace probes (left)
stack trace printed by above dtrace script (right)

PUBLIC

```
rasmus — lldb --wait-for --attach-name Archive Utility ▸ Archive Utility — 169×48
1: name = '_qtn_file_apply_to_path', locations = 1, resolved = 1, hit count = 2
  1.1: where = libquarantine.dylib`_qtn_file_apply_to_path, address = 0x00007fff6dbdd13b, resolved, hit count = 2

(lldb) br com add 1.1
Enter your debugger command(s).  Type 'DONE' to end.
> x -f s $rdi
> x -f s $rsi
(lldb) cont
Process 1719 resuming
(lldb)  x -f s $rdi
0x7fb692d0e500: "q/0083;619e8b8e;Safari;56B96AD9-4476-4DA6-9E41-500407D617EE"

(lldb)  x -f s $rsi
0x7fb693061000: "/private/var/folders/3d/4gzq8yw97cz35_55yqpv3pyh0000gn/T/com.apple.fileprovider.ArchiveService/TemporaryItems/(A Document Being Saved By ArchiveService)
/.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"

Process 1719 stopped
* thread #8, stop reason = breakpoint 1.1
    frame #0: 0x00007fff6dbdd13b libquarantine.dylib`_qtn_file_apply_to_path
libquarantine.dylib`_qtn_file_apply_to_path:
->  0x7fff6dbdd13b <+0>: pushq  %rbp
    0x7fff6dbdd13c <+1>: movq   %rsp, %rbp
    0x7fff6dbdd13f <+4>: pushq  %r14
    0x7fff6dbdd141 <+6>: pushq  %rbx
Target 0: (Archive Utility) stopped.
(lldb)
Process 1719 resuming
(lldb)  x -f s $rdi
0x7fb692d0e500: "q/0083;619e8b8e;Safari;56B96AD9-4476-4DA6-9E41-500407D617EE"

(lldb)  x -f s $rsi
0x7fb693061000: "/private/var/folders/3d/4gzq8yw97cz35_55yqpv3pyh0000gn/T/com.apple.fileprovider.ArchiveService/TemporaryItems/(A Document Being Saved By ArchiveService)
/.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx/.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxx"

Process 1719 stopped
* thread #8, stop reason = breakpoint 1.1
    frame #0: 0x00007fff6dbdd13b libquarantine.dylib`_qtn_file_apply_to_path
libquarantine.dylib`_qtn_file_apply_to_path:
->  0x7fff6dbdd13b <+0>: pushq  %rbp
    0x7fff6dbdd13c <+1>: movq   %rsp, %rbp
    0x7fff6dbdd13f <+4>: pushq  %r14
    0x7fff6dbdd141 <+6>: pushq  %rbx
Target 0: (Archive Utility) stopped.
(lldb)
```

lldb session debugging Archive Utility process, with breakpoint in _qtn_file_apply_to_path

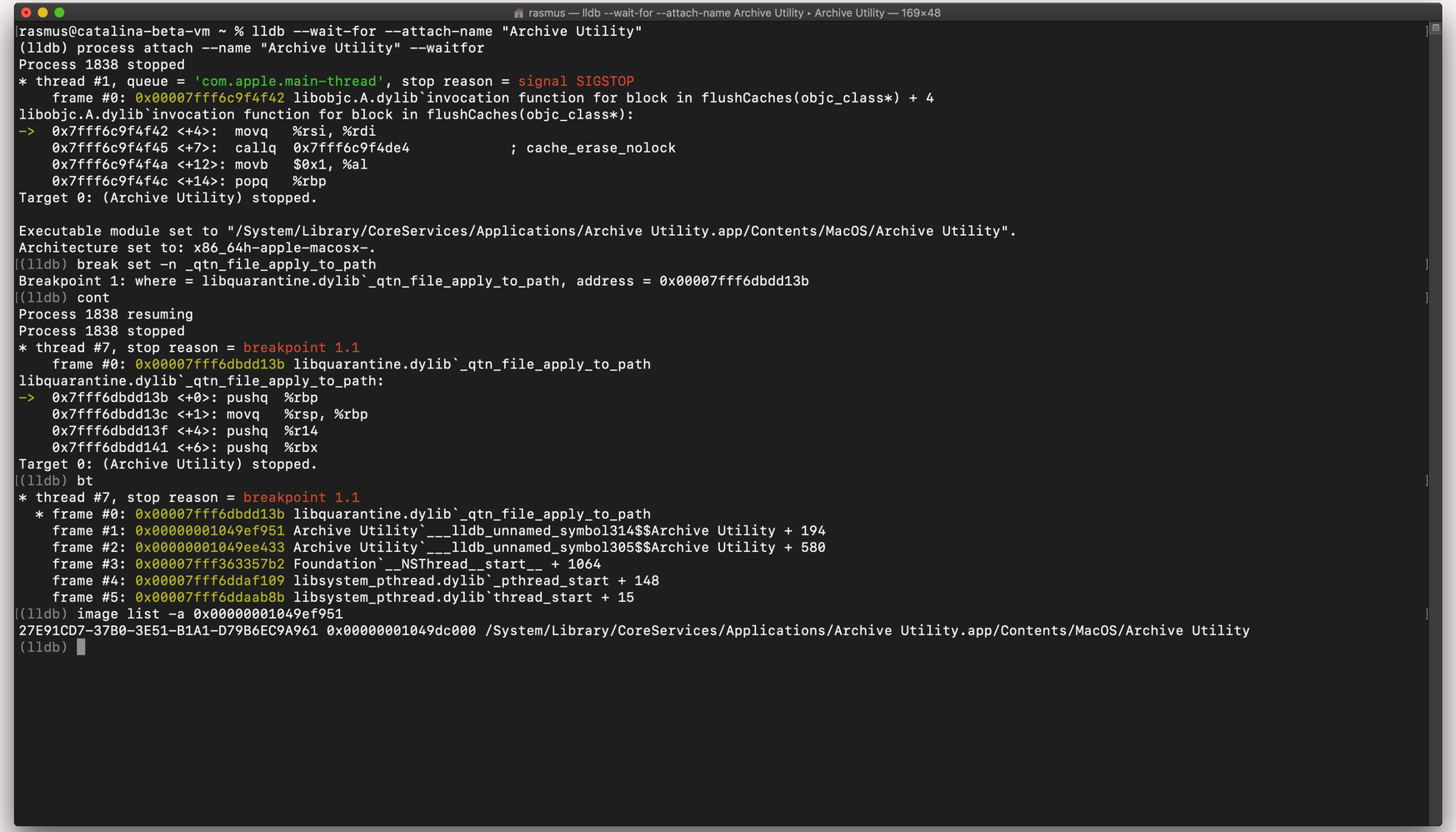
```
Process 1719 stopped
* thread #8, stop reason = breakpoint 1.1
    frame #0: 0x00007fff6dbdd13b libquarantine.dylib`_qtn_file_apply_to_path
libquarantine.dylib`_qtn_file_apply_to_path:
->  0x7fff6dbdd13b <+0>: pushq  %rbp
    0x7fff6dbdd13c <+1>: movq   %rsp, %rbp
    0x7fff6dbdd13f <+4>: pushq  %r14
    0x7fff6dbdd141 <+6>: pushq  %rbx
Target 0: (Archive Utility) stopped.
(lldb)
Process 1719 resuming
(lldb)  x -f s $rdi
0x7fb692d0e500: "q/0083;619e8b8e;Safari;56B96AD9-4476-4DA6-9E41-500407D617EE"

(lldb)  x -f s $rsi
0x7fb693061000: "/private/var/folders/3d/4gzq8yw97cz35_55yqpv3pyh0000gn/T/com.apple.fileprovider.ArchiveService/TemporaryItems/(A Document Being Saved By ArchiveService)
/.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx/.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxx/.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx/.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxx"

Process 1719 stopped
* thread #8, stop reason = breakpoint 1.1
    frame #0: 0x00007fff6dbdd13b libquarantine.dylib`_qtn_file_apply_to_path
libquarantine.dylib`_qtn_file_apply_to_path:
->  0x7fff6dbdd13b <+0>: pushq  %rbp
    0x7fff6dbdd13c <+1>: movq   %rsp, %rbp
    0x7fff6dbdd13f <+4>: pushq  %r14
    0x7fff6dbdd141 <+6>: pushq  %rbx
Target 0: (Archive Utility) stopped.
(lldb) setting set target.max-string-summary-length 2000
(lldb) x -f s $rsi
0x7fb693061000: "/private/var/folders/3d/4gzq8yw97cz35_55yqpv3pyh0000gn/T/com.apple.fileprovider.ArchiveService/TemporaryItems/(A Document Being Saved By ArchiveService)
/.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx/.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxx/.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx/.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
(lldb) cont
Process 1719 resuming
Process 1719 exited with status = 0 (0x00000000)
(lldb)
```

examining the arguments passed to qtn_file_apply_to_path()

- Archive Utility calls qtn_file_apply_to_path()
- This function fails when the pathname passed to it is >PATH_MAX
- Let’s reverse engineer the function that calls it



getting the image load address for the Archive Utility executable

```
/* @class BAHDecompressor */
-(void)_propagateQuarantineInformation {
    rdi = self;
    r12 = *ivar_offset(_qtInfo);
    COND = *(rdi + r12) == 0x0;
    if (!COND) {
            r14 = rdi;
            rax = _objc_msgSend_100027088();
            rax = [rax retain];
            rax = objc_retainAutorelease(rax);
            var_40 = [rax fileSystemRepresentation];
            *(&var_40 + 0x8) = 0x0;
            [rax release];
            rax = fts_open$INODE64(&var_40, 0x1c, 0x0);
            if (rax != 0x0) {
                    rbx = rax;
                    rax = fts_read$INODE64(rax, 0x1c, 0x0);
                    if (rax != 0x0) {
                            do {
                                    if (((*(int16_t *)(rax + 0x58) & 0xffff) <= 0xd) && (!COND)) {
                                            _qtn_file_apply_to_path(*(r14 + r12), *(rax + 0x28), 0x0);
                                    }
                                    rax = fts_read$INODE64(rbx);
                            } while (rax != 0x0);
                    }
                    fts_close$INODE64(rbx);
            }
    }
    if (**___stack_chk_guard != **___stack_chk_guard) {
            __stack_chk_fail();
    }
    return;
}
```

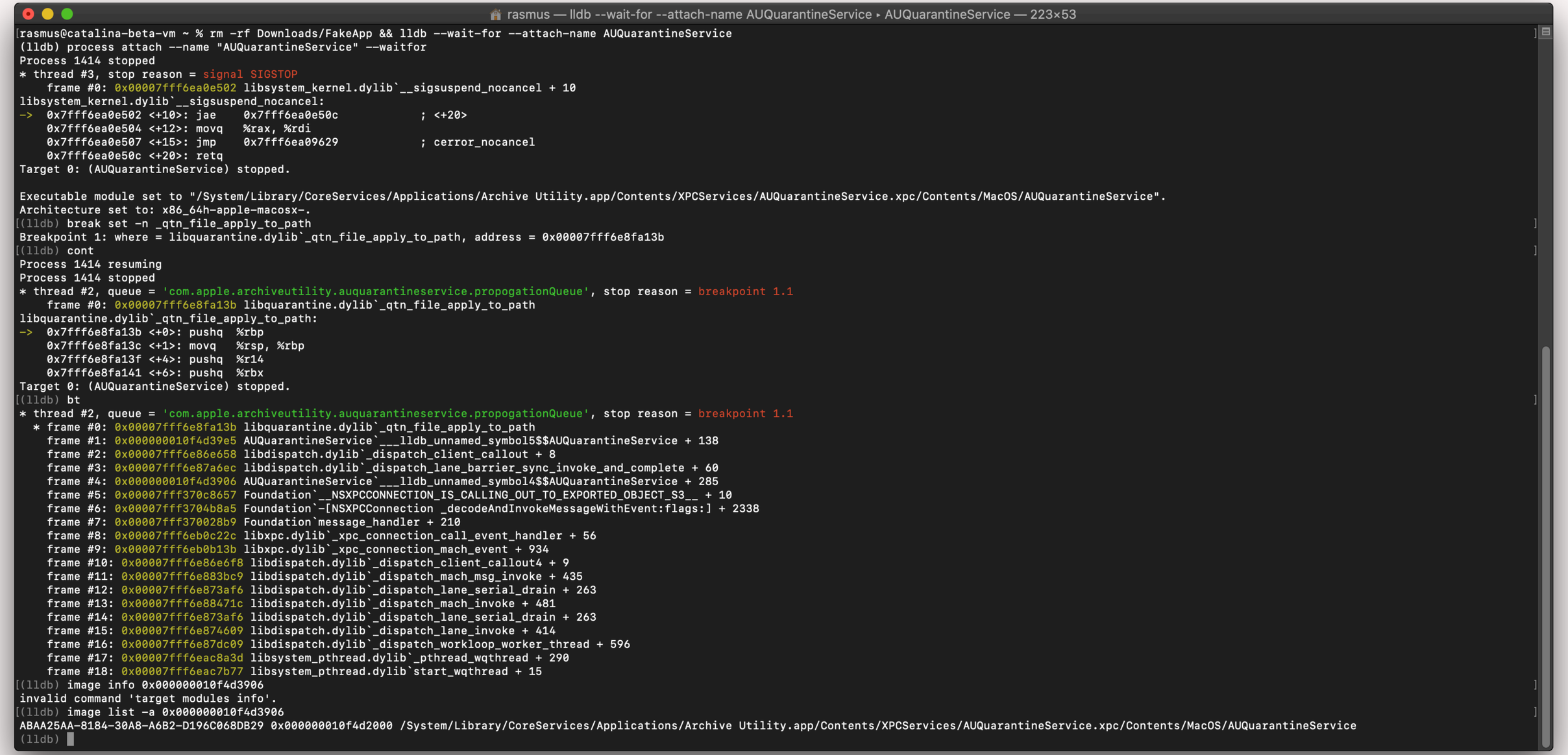
Hopper pseudo-code of function calling qtn_file_apply_to_path()

- Let’s used our DTrace script on a fixed version of macOS
- Ooh shiny, a new process called AUQuarantineService! Let’s take a look inside!

```
0 194885                vn_setxattr:entry
              kernel`mac_vnop_setxattr+0x105
              Quarantine`syscall_quarantine_setinfo_common+0x5e2
              Quarantine`syscall_quarantine_setinfo_path+0xd4
              kernel`__mac_syscall+0xee
              kernel`unix_syscall64+0x287
              kernel`hndl_unix_scall64+0x16

              libsystem_kernel.dylib`__mac_syscall+0xa
              libquarantine.dylib`_qtn_file_apply_to_path+0x68
              AUQuarantineService`0x0000000107b8195b+0x8a
              libdispatch.dylib`_dispatch_client_callout+0x8
              libdispatch.dylib`_dispatch_lane_barrier_sync_invoke_and_complete+0x3c
              AUQuarantineService`0x0000000107b817e9+0x11d
              Foundation`__NSXPCCONNECTION_IS_CALLING_OUT_TO_EXPORTED_OBJECT_S3__+0xa
              Foundation`-[NSXPCConnection _decodeAndInvokeMessageWithEvent:flags:]+0x922
              Foundation`message_handler+0xd2
              libxpc.dylib`_xpc_connection_call_event_handler+0x38
              libxpc.dylib`_xpc_connection_mach_event+0x3a6
              libdispatch.dylib`_dispatch_client_callout4+0x9
              libdispatch.dylib`_dispatch_mach_msg_invoke+0x1b3
              libdispatch.dylib`_dispatch_lane_serial_drain+0x107
              libdispatch.dylib`_dispatch_mach_invoke+0x1e1
              libdispatch.dylib`_dispatch_lane_serial_drain+0x107
              libdispatch.dylib`_dispatch_lane_invoke+0x19e
              libdispatch.dylib`_dispatch_workloop_worker_thread+0x254
              libsystem_pthread.dylib`_pthread_wqthread+0x122
              libsystem_pthread.dylib`start_wqthread+0xf
```

Output of the same Dtrace script on a fixed version of macOS



lldb session debugging AUQuarantineService, with breakpoint in _qtn_file_apply_to_path

```
int sub_10000195b(int arg0) {
    r14 = arg0;
    var_30 = [objc_retainAutorelease(*(arg0 + 0x20)) fileSystemRepresentation];
    *(&var_30 + 0x8) = 0x0;
    rax = fts_open$INODE64(&var_30, 0x18, 0x0);
    if (rax != 0x0) {
            rbx = rax;
            rax = fts_read$INODE64(rax, 0x18, 0x0);
            if (rax != 0x0) {
                    do {
                            if (((*(int16_t *)(rax + 0x58) & 0xffff) <= 0xd) && (!COND)) {
                                    _qtn_file_apply_to_path(*(r14 + 0x28), *(rax + 0x28), 0x0);
                            }
                            rax = fts_read$INODE64(rbx);
                    } while (rax != 0x0);
            }
            fts_close$INODE64(rbx);
    }
    var_20 = **___stack_chk_guard;
    rax = *___stack_chk_guard;
    rax = *rax;
    if (rax != var_20) {
            rax = __stack_chk_fail();
    }
    return rax;
}
```

Hopper pseudo-code of function calling qtn_file_apply_to_path() in a fixed version of macOS

rasmus — lldb --wait-for --attach-name AUQuarantineService ▸ AUQuarantineService — 223×53

```
    frame #16: 0x00007fff6e87dc09 libdispatch.dylib`_dispatch_workloop_worker_thread + 596
    frame #17: 0x00007fff6eac8a3d libsystem_pthread.dylib`_pthread_wqthread + 290
    frame #18: 0x00007fff6eac7b77 libsystem_pthread.dylib`start_wqthread + 15
(lldb) image info 0x000000010f4d3906
invalid command 'target modules info'.
(lldb) image list -a 0x000000010f4d3906
ABAA25AA-8184-30A8-A6B2-D196C068DB29 0x000000010f4d2000 /System/Library/CoreServices/Applications/Archive Utility.app/Contents/XPCServices/AUQuarantineService.xpc/Contents/MacOS/AUQuarantineService
(lldb)
(lldb)  x -f s $rdi
(lldb) x -f s $rsi
0x7f8f3c808a00: "/private/var/folders/3d/4gzq8yw97cz35_55yqpv3pyh0000gn/T/com.apple.fileprovider.ArchiveService/TemporaryItems/(A Document Being Saved By ArchiveService)"
(lldb) cont
Process 1414 resuming
Process 1414 stopped
* thread #2, queue = 'com.apple.archiveutility.auquarantineservice.propogationQueue', stop reason = breakpoint 1.1
    frame #0: 0x00007fff6e8fa13b libquarantine.dylib`_qtn_file_apply_to_path
libquarantine.dylib`_qtn_file_apply_to_path:
->  0x7fff6e8fa13b <+0>: pushq  %rbp
    0x7fff6e8fa13c <+1>: movq   %rsp, %rbp
    0x7fff6e8fa13f <+4>: pushq  %r14
    0x7fff6e8fa141 <+6>: pushq  %rbx
Target 0: (AUQuarantineService) stopped.
(lldb) x -f s $rsi
0x7f8f3bc0a3c8: "FakeApp.app"
(lldb) cont
Process 1414 resuming
Process 1414 stopped
* thread #2, queue = 'com.apple.archiveutility.auquarantineservice.propogationQueue', stop reason = breakpoint 1.1
    frame #0: 0x00007fff6e8fa13b libquarantine.dylib`_qtn_file_apply_to_path
libquarantine.dylib`_qtn_file_apply_to_path:
->  0x7fff6e8fa13b <+0>: pushq  %rbp
    0x7fff6e8fa13c <+1>: movq   %rsp, %rbp
    0x7fff6e8fa13f <+4>: pushq  %r14
    0x7fff6e8fa141 <+6>: pushq  %rbx
Target 0: (AUQuarantineService) stopped.
(lldb) x -f s $rsi
0x7f8f3bc0a448: ".xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
(lldb) cont
Process 1414 resuming
Process 1414 stopped
* thread #2, queue = 'com.apple.archiveutility.auquarantineservice.propogationQueue', stop reason = breakpoint 1.1
    frame #0: 0x00007fff6e8fa13b libquarantine.dylib`_qtn_file_apply_to_path
libquarantine.dylib`_qtn_file_apply_to_path:
->  0x7fff6e8fa13b <+0>: pushq  %rbp
    0x7fff6e8fa13c <+1>: movq   %rsp, %rbp
    0x7fff6e8fa13f <+4>: pushq  %r14
    0x7fff6e8fa141 <+6>: pushq  %rbx
Target 0: (AUQuarantineService) stopped.
(lldb) x -f s $rsi
0x7f8f3bd09cb8: ".xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
(lldb)
```

lldb session debugging AUQarantineService, examining arguments to qtn_file_apply_to_path()

```
[rasmus@catalina-beta-vm ~ % lsof -p 1414
lsof: WARNING: can't stat() vmhgfs file system /Volumes/VMware Shared Folders
      Output information may be incomplete.
      assuming "dev=33000002" from mount table
COMMAND    PID   USER   FD   TYPE DEVICE  SIZE/OFF                NODE NAME
AUQuarant 1414 rasmus  cwd    DIR    1,4        96         12885835620 /private/var/folders/3d/4gzq8yw97cz35_55yqpv3pyh0000gn/T/com.apple.fileprovider.ArchiveService/TemporaryItems/(A Document Being Saved By Archiv
eService)/.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
AUQuarant 1414 rasmus  txt    REG    1,4     37728 1152921500314092351 /System/Library/CoreServices/Applications/Archive Utility.app/Contents/XPCServices/AUQuarantineService.xpc/Contents/MacOS/AUQuarantineService
AUQuarant 1414 rasmus  txt    REG    1,4   1568368 1152921500314090500 /usr/lib/dyld
AUQuarant 1414 rasmus  txt    REG    1,4 2102263808         12885727253 /private/var/db/dyld/dyld_shared_cache_x86_64h
AUQuarant 1414 rasmus    0r   CHR    3,2       0t0                 310 /dev/null
AUQuarant 1414 rasmus    1u   CHR    3,2       0t0                 310 /dev/null
AUQuarant 1414 rasmus    2u   CHR    3,2       0t0                 310 /dev/null
AUQuarant 1414 rasmus    3r   DIR    1,4       320         12885831226 /Users/rasmus/Library/Containers/com.apple.archiveutility.auquarantineservice/Data
rasmus@catalina-beta-vm ~ %
```

lsof(8) output, showing current working directory (cwd) of AUQuarantineService process (top)
lldb session with breakpoint at chdir(), demonstrating where cwd is set (bottom)

rasmus — lldb --wait-for --attach-name AUQuarantineService ▸ AUQuarantineService — 223×53

```
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
[(lldb) cont
Process 1414 resuming
Process 1414 stopped
* thread #2, queue = 'com.apple.archiveutility.auquarantineservice.propogationQueue', stop reason = breakpoint 1.1
    frame #0: 0x00007fff6e8fa13b libquarantine.dylib`_qtn_file_apply_to_path
libquarantine.dylib`_qtn_file_apply_to_path:
->  0x7fff6e8fa13b <+0>: pushq  %rbp
    0x7fff6e8fa13c <+1>: movq   %rsp, %rbp
    0x7fff6e8fa13f <+4>: pushq  %r14
    0x7fff6e8fa141 <+6>: pushq  %rbx
Target 0: (AUQuarantineService) stopped.
[(lldb) x -f s $rsi
0x7f8f3bd09cb8: ".xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
[(lldb) break set -r chdir
Breakpoint 2: 8 locations.
[(lldb) cont
Process 1414 resuming
Process 1414 stopped
* thread #2, queue = 'com.apple.archiveutility.auquarantineservice.propogationQueue', stop reason = breakpoint 2.4
    frame #0: 0x00007fff6ea294fc libsystem_kernel.dylib`fchdir
libsystem_kernel.dylib`fchdir:
->  0x7fff6ea294fc <+0>:  movl   $0x200000d, %eax          ; imm = 0x200000D
    0x7fff6ea29501 <+5>:  movq   %rcx, %r10
    0x7fff6ea29504 <+8>:  syscall
    0x7fff6ea29506 <+10>: jae    0x7fff6ea29510            ; <+20>
Target 0: (AUQuarantineService) stopped.
[(lldb) bt
* thread #2, queue = 'com.apple.archiveutility.auquarantineservice.propogationQueue', stop reason = breakpoint 2.4
  * frame #0: 0x00007fff6ea294fc libsystem_kernel.dylib`fchdir
    frame #1: 0x00007fff6e91c35d libsystem_c.dylib`fts_safe_changedir + 90
    frame #2: 0x00007fff6e91c572 libsystem_c.dylib`fts_build + 477
    frame #3: 0x00007fff6e91c1dd libsystem_c.dylib`fts_read$INODE64 + 893
    frame #4: 0x000000010f4d39ed AUQuarantineService`___lldb_unnamed_symbol5$$AUQuarantineService + 146
    frame #5: 0x00007fff6e86e658 libdispatch.dylib`_dispatch_client_callout + 8
    frame #6: 0x00007fff6e87a6ec libdispatch.dylib`_dispatch_lane_barrier_sync_invoke_and_complete + 60
    frame #7: 0x000000010f4d3906 AUQuarantineService`___lldb_unnamed_symbol4$$AUQuarantineService + 285
    frame #8: 0x00007fff370c8657 Foundation`__NSXPCCONNECTION_IS_CALLING_OUT_TO_EXPORTED_OBJECT_S3__ + 10
    frame #9: 0x00007fff3704b8a5 Foundation`-[NSXPCConnection _decodeAndInvokeMessageWithEvent:flags:] + 2338
    frame #10: 0x00007fff370028b9 Foundation`message_handler + 210
    frame #11: 0x00007fff6eb0c22c libxpc.dylib`_xpc_connection_call_event_handler + 56
    frame #12: 0x00007fff6eb0b13b libxpc.dylib`_xpc_connection_mach_event + 934
```

```
rax = fts_open$INODE64(&var_30, 0x18, 0x0);
if (rax != 0x0) {
        rbx = rax;
        rax = fts_read$INODE64(rax, 0x18, 0x0);
        if (rax != 0x0) {
                do {
                        if (((*(int16_t *)(rax + 0x58) & 0xffff) <= 0xd) && (!COND)) {
                                _qtn_file_apply_to_path(*(r14 + 0x28), *(rax + 0x28), 0x0);
                        }
                        rax = fts_read$INODE64(rbx);
                } while (rax != 0x0);
        }
        fts_close$INODE64(rbx);
}
```

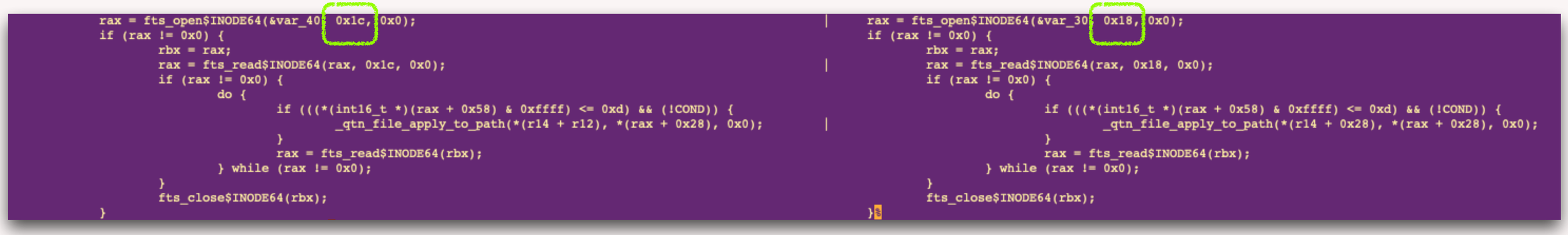
fixed version

```
rax = fts_open$INODE64(&var_40, 0x1c, 0x0);
if (rax != 0x0) {
        rbx = rax;
        rax = fts_read$INODE64(rax, 0x1c, 0x0);
        if (rax != 0x0) {
                do {
                        if (((*(int16_t *)(rax + 0x58) & 0xffff) <= 0xd) && (!COND)) {
                                _qtn_file_apply_to_path(*(r14 + r12), *(rax + 0x28), 0x0);
                        }
                        rax = fts_read$INODE64(rbx);
                } while (rax != 0x0);
        }
        fts_close$INODE64(rbx);
}
```

vulnerable version

```
rax = fts_open$INODE64(&var_40, 0x1c, 0x0);
if (rax != 0x0) {
        rbx = rax;
        rax = fts_read$INODE64(rax, 0x1c, 0x0);
        if (rax != 0x0) {
                do {
                        if (((*(int16_t *)(rax + 0x58) & 0xffff) <= 0xd) && (!COND)) {
                                _qtn_file_apply_to_path(*(r14 + r12), *(rax + 0x28), 0x0);
                        }
                        rax = fts_read$INODE64(rbx);
                } while (rax != 0x0);
        }
        fts_close$INODE64(rbx);
}
```

```
rax = fts_open$INODE64(&var_30, 0x18, 0x0);
if (rax != 0x0) {
        rbx = rax;
        rax = fts_read$INODE64(rax, 0x18, 0x0);
        if (rax != 0x0) {
                do {
                        if (((*(int16_t *)(rax + 0x58) & 0xffff) <= 0xd) && (!COND)) {
                                _qtn_file_apply_to_path(*(r14 + 0x28), *(rax + 0x28), 0x0);
                        }
                        rax = fts_read$INODE64(rbx);
                } while (rax != 0x0);
        }
        fts_close$INODE64(rbx);
}
```



```
rax = fts_open$INODE64(&var_40, 0x1c, 0x0);
if (rax != 0x0) {
        rbx = rax;
        rax = fts_read$INODE64(rax, 0x1c, 0x0);
        if (rax != 0x0) {
                do {
                        if (((*(int16_t *)(rax + 0x58) & 0xffff) <= 0xd) && (!COND)) {
                                _qtn_file_apply_to_path(*(r14 + r12), *(rax + 0x28), 0x0);
                        }
                        rax = fts_read$INODE64(rbx);
                } while (rax != 0x0);
        }
        fts_close$INODE64(rbx);
}
```

```
rax = fts_open$INODE64(&var_30, 0x18, 0x0);
if (rax != 0x0) {
        rbx = rax;
        rax = fts_read$INODE64(rax, 0x18, 0x0);
        if (rax != 0x0) {
                do {
                        if (((*(int16_t *)(rax + 0x58) & 0xffff) <= 0xd) && (!COND)) {
                                _qtn_file_apply_to_path(*(r14 + 0x28), *(rax + 0x28), 0x0);
                        }
                        rax = fts_read$INODE64(rbx);
                } while (rax != 0x0);
        }
        fts_close$INODE64(rbx);
}
```

side-by-side diff of vulnerable (left) and fixed (right) version

- According to its man page, the second argument to fts_open() is a bitmask of option flags
- Changed from 0x1c (…11100) to 0x18 (…11000)
- #define FTS_NOCHDIR 0x004 /* don't change directories */
- 0x1c - 0x18 = 0x4 (…00100)

Final thoughts

1. CVE-2023-27943
   - Relying just on one signal for activation of protection mechanisms (quarantine attribute) is not a bullet-proof solution
   - Apple should rethink the security approach and either introduce additional, more reliable metrics or a completely different security procedure for validation of content originated from the Internet. Otherwise, we will keep seeing similar security incidents.
   - It's also a good idea to test your changes against popular software on your platforms :). Especially when security incidents happen with pretty popular software like Google Chrome.
2. CVE-2021-1810
   - Two independent failures contributed to this:
     - Incorrect handling of deep directory hierarchies - operating system facilities for doing so are awkward and error prone
       - You need to either use chdir() which is a process-global state, or iterate using directory file descriptors
       - Many things in the operating system simply falls over when they encounter long file names
     - A variant of TOCTOU - quarantine attribute was applied in a different folder than the where the final result ended up, creating the sweet spot due to differences in the path prefixes
   - Archive Utility has other code paths calling qtn_file_apply_to_path() - my investigation was limited in scope to this particular use case
   - PATH_MAX and similar boundaries may be worth exploring further in the context of validation vs execution



F-Secure

Thank you!

More information:

- blog.f-secure.com/the-discovery-of-gatekeeper-bypass-cve-2021-1810/
- blog.f-secure.com/analysis-of-cve-2021-1810-gatekeeper-bypass/
- blog.f-secure.com/discovery-of-gatekeeper-bypass-cve-2023-27943/

Find us on social media:

Rasmus Sten <rasmus.sten@f-secure.com>
Mastodon/ActivityPub: @pajp@blog.dll.nu

Arthur Valiev <arthur.valiev@f-secure.com>
Twitter/X: @iBumerangArt